AOS-CX 10.11 Update

Certificate Enrollment using EST via Config Distribution

aruba
a Hewlett Packard Enterprise company

Shobana Nandakumar
Technical Marketing Engineer

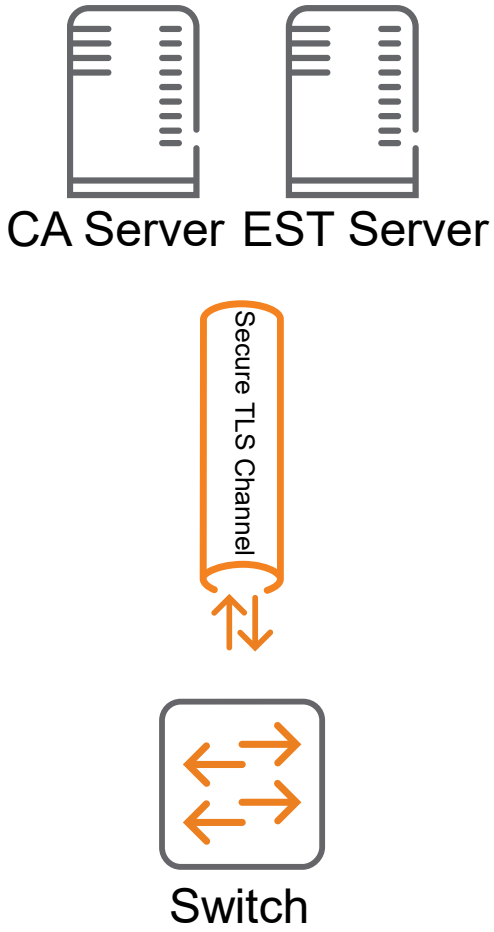
Agenda

1. Overview
2. Use Cases
3. Details and Caveats
4. Configuration
5. Best Practices
6. Troubleshooting
7. Demo
8. Additional Resources

Overview

EST

- EST stands for Enrollment over Secure Transport. It defines the protocol that devices use to request trusted CA (certificate authority) certificates and to enroll/re-enroll certificates from CA services via secure channels automatically
- An EST client is implemented as a part of the PKI infrastructure in the AOS-CX system.
- EST client on AOS-CX uses HTTP over TLS. It relies on the availability of TCP network, DNS service, and EST services reachable from the host AOS-CX switch.



Certificate Enrollment using EST via Config Distribution

- Certificate Enrollment via EST is performed using CLI and REST
- Certificate parameters and EST profile association does not reside in switch configuration
- Enhancements
  - Certificate Enrollment through config distribution – TFTP/SFTP/SCP/Net Edit/Central
  - Certificates parameters and EST profile association reside in switch configuration

Prior to 10.11

```
AOS-CX(config)# show version
--------------------------------------------------------------------------------
ArubaOS-CX
(c) Copyright 2017-2022 Hewlett Packard Enterprise Development LP
--------------------------------------------------------------------------------
Version      : FL.10.10.1000
Build Date   : 2022-08-15 17:37:25 UTC
Build ID     : ArubaOS-CX:FL.10.10.1000:cce338479a9d:202208151621
Build SHA    : cce338479a9d4ff4385ab15ca4863def0fea0fcc
Hot Patches  :
Active Image : primary

Service OS Version : FL.01.11.0001-internal
BIOS Version       : FL.01.0004
AOS-CX(config)# show run | in "crypto pki certificate"
AOS-CX(config)#
```

10.11 Onwards

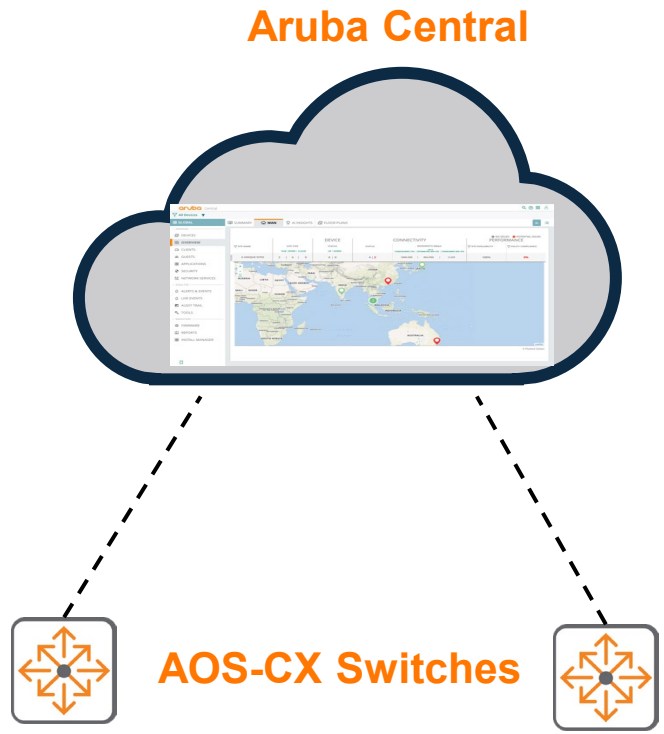
```
AOS-CX(config)# show version
--------------------------------------------------------------------------------
ArubaOS-CX
(c) Copyright 2017-2022 Hewlett Packard Enterprise Development LP
--------------------------------------------------------------------------------
Version      : FL.10.11.0001U
Build Date   : 2022-08-30 10:30:19 UTC
Build ID     : ArubaOS-CX:FL.10.11.0001U:b7d5680686b1:202208300908
Build SHA    : b7d5680686b1857e2d5a8a600b3c5e7f66ea54ab
Hot Patches  :
Active Image : secondary

Service OS Version : FL.01.11.0001-internal
BIOS Version       : FL.01.0004
AOS-CX(config)# show run | begin "crypto pki certificate"
crypto pki certificate est_enrollment_certificate
    subject common-name est-cert
    enroll est-profile cppm
```

Use Cases

Use Cases

- Switches can enroll and re-enroll certificates automatically instead of manual enrollment via CLI/REST
- ZTP
  - Central can push PKI configurations for enrollment
- Customers can select their own PKI infrastructure
- Common supported service certificates in AOS-CX
  - Syslog
  - HTTPs
  - Captive Portal
  - RADSec
  - Dot1x-Supplicant
  - EST-Client
  - Hardware Switch Controller



Details

EST Details

- The EST client in the AOS-CX operating system requires configuration to create EST profiles, each including an EST server URL, and the name of the VRF in which HTTP connection to the EST server can be established.
- At the time a user provides an URL for an EST profile, the EST client will try to contact the EST server and download the trusted CA certificate set. The trusted CA certificate set will also be downloaded right before a certificate enrollment or re-enrollment is made, in order to accommodate possible update to the CA certificates.
- The Certificate enrollment user interface offers a parameter of EST profile name. When such parameter is provided, PKI (Certificate Manager) will call the EST client to perform the certificate enrollment.
- The current PKI implementation on AOS-CX supports up to:
  - 16 EST profiles
  - 63 trusted CA certificates
  - 18 certificates

Certificate Enrollment using EST via Config Distribution

Certificate Enrollment using EST via Config Distribution is supported via following channels

Methods -

- CLI
- JSON

Applications/Protocols-

- TFTP
- SFTP
- SCP
- USB
- Checkpoint
- Central
- NetEdit

Configuration

Prerequisite for Certificate Enrollment via EST

- Establish the PKI infrastructure for the enterprise, with the CA chain and service ready to issue certificate. Issue a service certificate for the EST server. Optionally, issue a client certificate for the EST client.

- Provide the root CA certificate in a TA profile on the Aruba CX switch that will validate the EST server certificate in the config file -

```
crypto pki ta-profile <ta-name>
ta-certificate
-----BEGIN CERTIFICATE-----
------------------------
-----END CERTIFICATE-----
```

- Establish the EST server reachable from the Aruba CX switch. Connect the CA service(s) to the EST server. If there is client certificate for the EST client, install the root CA certificate on the server that will validate the client certificate.

EST Profile Configuration

In the global configuration context, create an EST profile and enter its context:

```
crypto pki est-profile <est-name>
```

In an EST profile context, configure the EST profile parameters:

```
url <URL>
vrf <VRF>
username <USER> password [ciphertext <PASSWORD> | plaintext <PASSWORD>]
retry-interval <SECONDS>
retry-count <COUNT>
arbitrary-label <LABEL>
arbitrary-label-enrollment <LABEL>
arbitrary-label-reenrollment <LABEL>
reenrollment-lead-time <DAYS>
```

Certificate Enrollment Configuration

In the global configuration context, create a certificate profile and enter its context:

```
crypto pki certificate <cert-name>
```

In a certificate profile configuration context, configure the certificate parameters:

```
key-type {rsa [key-size <size>] | ecdsa [curve-size <size>]}
subject [common-name <common-name>]
        [country <country>]
        [locality <locality>]
        [org <organization>]
        [org-unit <org-unit>]
        [state <state>]
```

In a certificate configuration context, enroll the certificate via an EST service:

```
enroll est-profile <est-name>
```

Sample Config in CLI and JSON

CLI

```
crypto pki ta-profile est_ta_profile
    ta-certificate
        -----BEGIN CERTIFICATE-----
        MIIEfzCCA2egAwIBAgIBAzANBgkqhkiG9w0BAQ0FADCBxjELMAkGA1UEBhMCVVMx
        AQEFAAOCAQ8AMIIBCgKCAQEA2dwJBCwi1ymOou6UPY0KW1bvpbBN8PBqNbMhW1Y6
        p65lCpFIXWJfmcCGG8xd4AtBJLGm1EqmdTj2hDYpI+UXXuJa00GCuamiQhxFRuTk
        Sf3XZHQIc7hcpvtUM2tmHn9nHt3/qE04789Y0OSKGfyr2Zzrv6VSzRw3KSaGLKKW
        LaYlkjSNzQ1Ig8l0TL8DInDXcLORLXykOBrpDG/y1x3EKtsyzqB0CAvJt4NEo2dQ
        cZFmVl+pSrCt2oEx+FMnGbbARAYp7dxSRTItkWd/gOHEL1r7qozZFPPa47t3lhbx
        oYdFBScTUWxDPsx+MIjnZ1ijuuOfJuBBIl9Ag6Y0BmdgSwIDAQABo3YwdDAdBgNV
        HQ4EFgQUYjAjx8mhfcyTOBVrv0QmqDDoYmEwDwYDVR0PAQH/BAUDAweGADAPBgNV
        HRMBAf8EBTADAQH/MDEGA1UdJQQqMCgGCCsGAQUFBwMJBggrBgEFBQcDAgYIKwYB
        BQUHAwEGCCsGAQUFBwMDMA0GCSqGSIb3DQEBDQUAA4IBAQC+ZRbUMkJPOeIQSPUd
        8WViFuHxb6yEOiieNbNxW58AfovbEJ7TWMeppoFvg8G66z4SFMb3zXN8iBEhCMJZ
        g99nGnO98BzgKAb3IlGomwFP0rRAmKYbreC5m8Bw7PsqpSzKNhGUiMaPB7L8Vw/4
        0ivzGhk7/a0hhmjM40/wUy03uvlAWfZs6hD3ALZIBJE23Pb3akkMxmGHy3G1zc63
        I9ngQQQMMq3XrCdW3VPEVZQYC+4R1RDjQD7z4hLPK69cLlp1aeuxBvTRMoCEfBmj
        m2PPsOWbVZizUxhR+4YoirZxTUQ9rjuk2cvuEEl4UMUQ1LZXlwjbar5z6BG22TdW
        RUqk
        -----END CERTIFICATE-----
        END_OF_CERTIFICATE
crypto pki est-profile est-sample-profile
    url https://cppm.tmelab.net/.well-known/est/ca:2
    username tester password ciphertext AQBapdW8I162MmfOUhNaa7xpBmuxa6MZMP
crypto pki certificate est-sample-cert
    subject common-name est-sample-cert
    enroll est-profile est-sample-profile
```

JSON

```
    "PKI_EST_Profile": {
        "est-sample-profile": {
            "name": "est-sample-profile",
            "password": "AQBapdW8I162MmfOUhNaa7xpBmuxa6MZMPjY0vCYWij0RUBCCQAAAJLZFgeOj+2O1A==",
            "url": "https://cppm.tmelab.net/.well-known/est/ca:2",
            "username": "tester"
        }
    },
    "PKI_TA_Profile": {
        "est_ta_profile": {
            "certificate": "-----BEGIN CERTIFICATE-----\nMIIEfzCCA2egAwIBAgIBAzANBgkqhkiG9w0BAQ0
kNhbGlmb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTEXMBUGA1UE\nCgwOQXJ1YmEgTmV0d29ya3MxNDAyBgNVBAMMK0VTVCE
SBBdXRob3JpdHkxPzA9BgkqhkiG9w0BCQEWMDBmOGUwNzFm\nLWEyMTMtNDY2YS1hNDM0LTc4MjllYjg5ZTA0NUBleGFtcGx
zAwOTIzMzFaMIHGMQswCQYDVQQGEwJVUzETMBEGA1UE\nCAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJU3Vubnl2YWxlMRcwFQY
wwrRVNUIENsZWFyUGFzcyBPbmJvYXJkIENlcnRp\nZmljYXRlIEF1dGhvcml0eTE/MD0GCSqGSIb3DQEJARYwMGY4ZTA3MWY
GV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0B\nAQEFAAOCAQ8AMIIBCgKCAQEA2dwJBCwi1ymOou6UPY0KW1bvpbBN8PBqNbM
Tj2hDYpI+UXXuJa00GCuamiQhxFRuTk\nSf3XZHQIc7hcpvtUM2tmHn9nHt3/qE04789Y0OSKGfyr2Zzrv6VSzRw3KSaGLKK
G/y1x3EKtsyzqB0CAvJt4NEo2dQ\ncZFmVl+pSrCt2oEx+FMnGbbARAYp7dxSRTItkWd/gOHEL1r7qozZFPPa47t3lhbx\nc
mdgSwIDAQABo3YwdDAdBgNV\nHQ4EFgQUYjAjx8mhfcyTOBVrv0QmqDDoYmEwDwYDVR0PAQH/BAUDAweGADAPBgNV\nHRMBA
ggrBgEFBQcDAgYIKwYB\nBQUHAwEGCCsGAQUFBwMDMA0GCSqGSIb3DQEBDQUAA4IBAQC+ZRbUMkJPOeIQSPUd\n8WViFuHxb
Mb3zXN8iBEhCMJZ\ng99nGnO98BzgKAb3IlGomwFP0rRAmKYbreC5m8Bw7PsqpSzKNhGUiMaPB7L8Vw/4\n0ivzGhk7/a0hh
mGHy3G1zc63\nI9ngQQQMMq3XrCdW3VPEVZQYC+4R1RDjQD7z4hLPK69cLlp1aeuxBvTRMoCEfBmj\nm2PPsOWbVZizUxhR-
BG22TdW\nRUqk\n-----END CERTIFICATE-----",
            "name": "est_ta_profile"
        }
    },
    "PKI_X509_Certificate": {
        "est_enrollment_certificate": {
            "common_name": "est-sample-cert",
            "est_profile": "est-sample-profile",
            "name": "est_sample-cert"
        }
```

Show Commands

Show the list of EST profiles or the detail of an EST profile:

```
show crypto pki est-profile [<est-name>]
```

Each CA certificate downloaded from an EST server will be stored in a TA profile, with a TA profile name <est-name>-est-taNN, where NN is a two-digit sequence number. To show the list of TA profiles (including both user-configured and EST-downloaded), or the detail of an TA profile:

```
show crypto pki ta-profile [<ta-name>]
```

Show the list of certificates (including those manually enrolled and EST-enrolled), or the detail of a certificate：

```
show crypto pki certificate [<cert-name>]
```

Show the certificate associated with EST client for authentication:

```
show crypto pki application
```

Best Practices

Feature Best Practices

- Make sure DNS entries are resolved and EST server is reachable via the correct port
- Ensure the time is synchronized on both the Aruba CX switch (the EST client) and the EST server
- The EST server should include not only the root CA certificate, but also the intermediate issuer CA certificates, in the trusted CA certificate set that will be sent to the client upon request.
- If there is plan to delete the certificate , make sure configuration is removed from the saved config files or else after reboot the certificate will be enrolled again.

Troubleshooting

Troubleshooting Tips

EST client implementation on AOS-CX has very good debug logging messages. Make sure you enable it at the debug level so that you get the most details:

```
debug pki all [severity debug]
debug destination {buffer|console|syslog} [severity debug]
```

For NetEdit and Central debugging :

```
debug rest all [severity debug]
debug central all [severity debug]
```

Some common issues:

- **Cannot connect to EST server**
  - Cannot resolve the server domain name – DNS service not reachable
  - Connection rejected – TCP port correct?
- **CA certs request fails**
  - Server URL correct? Include “/.well-known/est”?
  - Server certificate invalid - root CA certificate for server installed on switch? SAN/CN matches host name? cert purpose set appropriately?
  - All intermediate CA certificates and server certificate have required fields?
- **Enrollment fails**
  - Username/password in EST profile correct? Or Certificate for EST client set correctly?
  - Certificate not yet valid – client and server clock sync’d?

Resources

Feature References

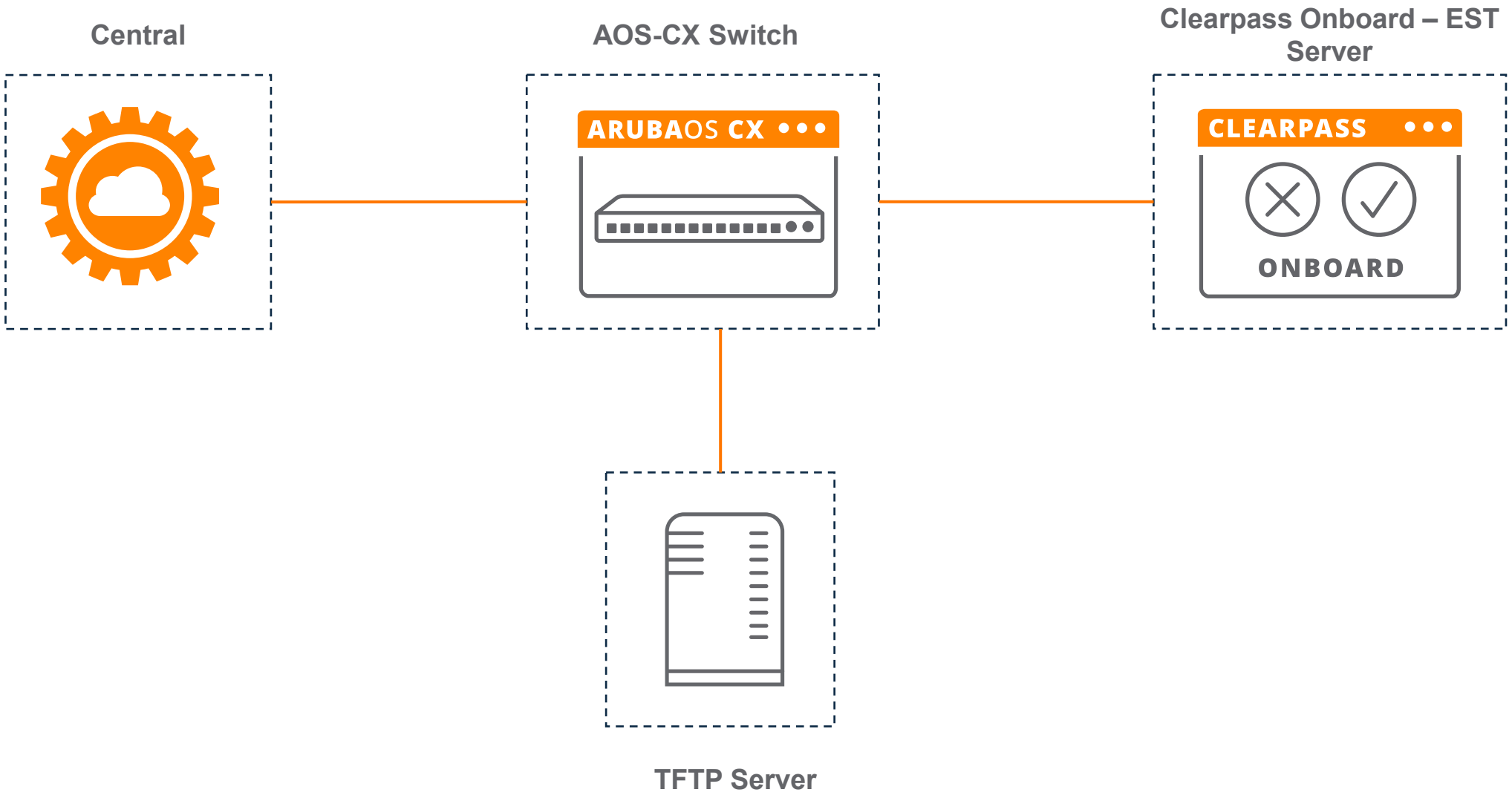
– RFC 5280: https://tools.ietf.org/html/rfc5280

– RFC 7030: https://tools.ietf.org/html/rfc7030

– EST Implementation in AOS-CX - https://www.youtube.com/watch?v=ZWVt-cNSEso

Demo

Topology


Central
AOS-CX Switch
Clearpass Onboard – EST Server
ARUBAOS CX
CLEARPASS
ONBOARD
TFTP Server

aruba
a Hewlett Packard Enterprise company

Thank you

shobana.nandakumar@hpe.com