Sinh chứng chỉ ActiveMQ keystores.

- ActiveMQ cho phép sử dụng 3 loại CA, trong bài sẽ sử dụng lại chứng chỉ có sẵn của Puppet CA. (xem thêm tại docs)

Yếu cầu trước khi cấu hình:

- Lấy đường dẫn chứng chỉ PuppetCA (thuộc PuppetMaster)

# puppet agent --configprint ssldir

- Các chứng chỉ sẽ sử dụng lại (có thể copy ra 1 thư mục khác):

+ <ssldir>/certs/ca.pem

+ <ssldir>/certs/<node name>.pem

+ <ssldir>/private\_keys/<node name>.pem

Note (quan trọng):

+ <node name> là chứng chỉ sẽ được sử dụng lại, nó phải là chứng chỉ của node cấu hình activeMQ:

+ VD: activeMQ được cài trên node “master.puppet.local” => nó phải sử dụng chứng chỉ của “master.puppet.local.pem” cho việc chứng thực activeMQ.

Cấu hình tạo Keystores:

- Trong phần sẽ cấu hình 2 chứng chỉ “truststore” và “keystore” (2 file đều có passwd, nên dùng chung cho dễ nhớ, nó sẽ được sử dụng để cấu hình activeMQ)

Bước 1: Cấu hình Truststore

- Nó sẽ yêu cầu CA-verified TLS.

- Nó sử dụng để làm rõ những chứng chỉ nào sẽ được kết nối tới ActiveMQ. Nếu sử dụng CA cert để tạo truststore, nó sẽ cho phép tất cả chứng chỉ được ký bởi CA.

- Tạo chứng chỉ từ file “.pem”

- Câu lệnh tạo chứng chỉ:

keytool -import -alias "My CA" -file ca.pem -keystore truststore.jks

Enter keystore password:

Re-enter new password:

…..

Trust this certificate? [no]: y

Certificate was added to keystore

- Kiểm tra lại:

$ keytool -list -keystore truststore.jks

Enter keystore password:

Keystore type: JKS

Keystore provider: SUN

Your keystore contains 1 entry

my ca, Mar 30, 2012, trustedCertEntry,

Certificate fingerprint (MD5): 99:D3:28:6B:37:13:7A:A2:B8:73:75:4A:31:78:0B:68

$ openssl x509 -in ca.pem -fingerprint -md5

MD5 Fingerprint=99:D3:28:6B:37:13:7A:A2:B8:73:75:4A:31:78:0B:68

Bước 2: Tạo Keystore:

- Keystore chứa chứng chỉ ActiveMQ broker’s và private key, nó sử được sử dụng để cho phép node cấu hình ActiveMQ middleware được quyền kết nối vào ActiveMQ.

- Theo bài hướng dẫn, ta cài đặt ActiveMQ trên node “master.puppet.local” => ta sẽ sử dụng chứng chỉ “master.puppet.local”.

- Tạo chứng chỉ:

$ sudo cat activemq\_private.pem activemq\_cert.pem > temp.pem

$ sudo openssl pkcs12 -export -in temp.pem -out activemq.p12 -name master.puppet.local

Enter Export Password:

Verifying - Enter Export Password:

$ sudo keytool -importkeystore -destkeystore keystore.jks -srckeystore activemq.p12 -srcstoretype PKCS12 -alias master.puppet.local

Enter destination keystore password:

Re-enter new password:

Enter source keystore password:

- Kiểm tra lại:

$ sudo keytool -list -keystore keystore.jks

Enter keystore password:

Keystore type: JKS

Keystore provider: SUN

Your keystore contains 1 entry

master.puppet.local, , PrivateKeyEntry,

Certificate fingerprint (MD5): 7E:2A:B4:4D:1E:6D:D1:70:A9:E7:20:0D:9D:41:F3:B9

$ sudo openssl x509 -in activemq\_cert.pem -fingerprint -md5

MD5 Fingerprint=7E:2A:B4:4D:1E:6D:D1:70:A9:E7:20:0D:9D:41:F3:B9

Bước 3:

- Nhớ vị trí lưu “keystore.jks” và “truststore.jks”. 2 chứng chỉ này sẽ được sử dụng cho cấu hình ssl activeMQ.

e