Nâng cấp chứng thực giữa Mcollective Client và Mcollective Server

- Default cơ chế chứng thực sử dụng “psk”

- Các cơ chế được hỗ trợ: ssl, psk, aes\_security và 1 số phần mềm thứ 3.

- Trong bài, ta sẽ nâng cấp cơ chế chứng thực bằng SSL Plugin.

Yêu cầu trước khi cài đặt:

- Đã cài đặt ActiveMQ

- Đã cài đặt Mcollective (ko ssl hoặc đã có ssl)

- Bài sẽ tận dụng cấu hình có sẵn khi cấu hình mcollective (Đã cấu hình ssl)

SSL Plugin Settings

Note:

+ Cơ chế này đòi hỏi bạn phải kiểm soát và phần phối chứng chỉ SSL

+ Tất cả server sẽ chia sẻ 1 cặp khóa “keypair”, sử dụng chung trên tất cả server.- Sẽ phải copy public key và private key

+ Tất cả admin user sẽ sử dụng chung server public key.

+ Tất cả admin user sẽ có 1 cặp khóa riêng

+ Tất cả server sẽ phải copy tất cả khóa public của tất cả client muốn kết nối

- Tất cả các tùy chọn đều không có giá trị mặc định, chung phải được set.

Tại server:

Bước 1:

- Cấu hình tại file server.cfg

- Ý nghĩa các cấu hình (xem giải thích trong cấu hình mcollective các phần trước)

- Xem chi tiết hơn tại file cấu hình mẫu

main\_collective = mcollective

collectives = mcollective

libdir = /opt/puppetlabs/mcollective/plugins

# consult the "classic" libdirs too

libdir = /usr/share/mcollective/plugins

libdir = /usr/libexec/mcollective

logfile = /var/log/puppetlabs/mcollective/mcollective.log

loglevel = info

daemonize = 1

# Plugins

# cấu hình sử dụng ssl plugin

securityprovider = ssl

# đường dẫn nơi chưa thư mục các key public mcollective client

plugin.ssl\_client\_cert\_dir = /etc/puppetlabs/puppet/ssl/certs/

# Đường dẫn cặp khóa server (dùng chung trên tất cả server)

plugin.ssl\_server\_private = /etc/puppetlabs/puppet/ssl/private\_keys/master.puppet.local.pem

plugin.ssl\_server\_public = /etc/puppetlabs/puppet/ssl/certs/master.puppet.local.pem

#####

connector = activemq

plugin.activemq.pool.size = 1

plugin.activemq.pool.1.host = master.puppet.local

plugin.activemq.pool.1.port = 61614

plugin.activemq.pool.1.user = mcollective

plugin.activemq.pool.1.password = marionette

#####

plugin.activemq.pool.1.ssl = 1

plugin.activemq.pool.1.ssl.ca = /etc/puppetlabs/puppet/ssl/certs/ca.pem

plugin.activemq.pool.1.ssl.cert = /etc/puppetlabs/puppet/ssl/certs/master.puppet.local.pem

plugin.activemq.pool.1.ssl.key = /etc/puppetlabs/puppet/ssl/private\_keys/master.puppet.local.pem

plugin.activemq.pool.1.ssl.fallback = 0

plugin.activemq.stomp\_1\_0\_fallback = 0

plugin.activemq.heartbeat\_interval = 30

plugin.activemq.max\_hbread\_fails = 2

plugin.activemq.max\_hbrlck\_fails = 0

# Facts

factsource = yaml

plugin.yaml = /etc/puppetlabs/mcollective/facts.yaml

Bước 2:

- Reset lại Mcollective

systemctl restart mcollective

Tại client:

Bước 1:

- Truy cập file client.cfg

- Xem chi tiết hơn tại file cấu hình mẫu

main\_collective = mcollective

collectives = mcollective

libdir = /opt/puppetlabs/mcollective/plugins

# consult the "classic" libdirs too

libdir = /usr/share/mcollective/plugins

libdir = /usr/libexec/mcollective

logger\_type = console

loglevel = warn

# Plugins

securityprovider = ssl

# Khóa public của server (tất cả server dùng chung)

plugin.ssl\_server\_public = /etc/puppetlabs/puppet/ssl/certs/master.puppet.local.pem

# Cặp khóa của client (Đã được mcollective server quản lý)

plugin.ssl\_client\_private = /etc/puppetlabs/puppet/ssl/private\_keys/activemq.pem

plugin.ssl\_client\_public = /etc/puppetlabs/puppet/ssl/certs/activemq.pem

#####

connector = activemq

plugin.activemq.pool.size = 1

plugin.activemq.pool.1.host = master.puppet.local

plugin.activemq.pool.1.port = 61614

plugin.activemq.pool.1.user = mcollective

plugin.activemq.pool.1.password = marionette

#####

plugin.activemq.pool.1.ssl = 1

plugin.activemq.pool.1.ssl.ca = /etc/puppetlabs/puppet/ssl/certs/ca.pem

plugin.activemq.pool.1.ssl.cert = /etc/puppetlabs/puppet/ssl/certs/activemq.pem

plugin.activemq.pool.1.ssl.key = /etc/puppetlabs/puppet/ssl/private\_keys/activemq.pem

plugin.activemq.pool.1.ssl.fallback = 0

plugin.activemq.stomp\_1\_0\_fallback = 0

plugin.activemq.heartbeat\_interval = 30

plugin.activemq.max\_hbread\_fails = 2

plugin.activemq.max\_hbrlck\_fails = 0

connection\_timeout = 3

Bước 2:

- Restart lại service mcollective

systemctl restart mcollective

e