Triển khai Mcollective với SSL, TLS, CA

- Cấu hình Mcollective với SSL, TLS, bảo mật mức transport level và application level.

Yêu cầu trước khi cài đặt:

- Đã triển khai trước activeMQ

- Đã triển khai mô hình puppet agent/master

- Đã đọc cấu hình Mcollective đơn giản, không sử dụng SSL, TLS, CA hoặc đã triển khai Mcollective không sử dụng ssl, tls, ca.

Note:

- Trong hướng dẫn, activeMQ được cài cùng puppet master

Yêu cầu cho cài đặt:

- Làm rõ các chứng chỉ sẽ sử dụng

|  |  |
| --- | --- |
| Credential | Used By: |
| ActiveMQ username/password | Middleware, servers, clients |
| CA certificate | Middleware, servers, clients |
| Signed certificate and private key for ActiveMQ | Middleware |
| Signed certificate and private key for each server | Servers |
| Signed certificate and private key for each user | Clients (both parts), servers (certificate only) |
| Shared server public and private key | Servers (both parts), clients (public key only) |

- Giải thích:

+ ActiveMQ user/passwd: là user, passwd có quyền truy cập vào activeMQ

+ Các chứng chỉ sẽ được sử dụng lại từ Puppet Master/CA

Cấu hình Middleware (sử dụng activeMQ)

Bước 1:

- Cấu hình activeMQ (Trong tài liệu hướng dẫn)

Note:

+ Sử dụng activeMQ 5.15

Bước 2:

- Thay đổi và nhớ passwd user được quyền truy cập vào activeMQ, ở đây sẽ vẫn giữa passwd mặc định

|  |
| --- |
| <users>  <authenticationUser username="mcollective" password="marionette" groups="mcollective,everyone"/>  <authenticationUser username="admin" password="secret" groups="mcollective,admins,everyone"/>  </users> |

Bước 3:

- Chỉnh port và protocol kết nối tới middleware, trong bài activeMQ sử dụng > 5.9

|  |  |
| --- | --- |
| <transportConnector name="stomp+nio" uri="stomp+nio://0.0.0.0:61613"/> | <transportConnector name="stomp+nio+ssl" uri="stomp+nio+ssl://0.0.0.0:61614?needClientAuth=true"/> |

Bước 4:

- Sinh chứng chỉ ActiveMQ Keystores, sử dụng các chứng chỉ có sẵn của Puppet CA

- Xem hướng dẫn sinh chứng chỉ keystores

Bước 5:

- Chỉnh sửa file activemq.xml. Thêm tag “sslContext”.

- Xem hướng dẫn “cấu hình activeMQ sử dụng sslContext”

Bước 6:

- Restart ActiveMQ service.

Bước 7:

- Chắc chắn port 61614 đã mở.

Cấu hình Mcollective Server và Mcollective Clients

Tại server:

- Cấu hình tại file server.cfg

- Cấu hình server.cfg gần như giống với cấu hình Mcollective ko ssl

- Xem chi tiết hơn tại folder “cấu hình mẫu”

vi /etc/puppetlabs/mcollective/server.cfg

……

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

securityprovider = psk

plugin.psk = unset

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

#####

# = 1 khi sử dụng ssl tls

plugin.activemq.pool.1.ssl = 1

# chứng chỉ CA sử dụng khi tạo truststore.jks

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

# Đây phải là chứng chỉ node triển khai activeMQ

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

# Đây phải là chứng chỉ node triển khai activeMQ

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

Tại client:

- Cấu hình file client.cfg

- Cấu hình client trong Mcollective, nó gần giống file server.cfg

vim /etc/puppetlabs/mcollective/client.cfg

….

####

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 = psk

plugin.psk = unset

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

Note:

- Reset lại service Mcollective khi cấu hình thay đổi file client.cfg và server.cfg

systemctl status mcollective

Note:

- Có thể cấu hình đồng thời client và server trong cùng 1 node.

- “plugin.psk = changemeplease” và “securityprovider = psk” phải trùng trên tất cả các server và client để middleware có thể nhận diện được các node.

- Xem thêm tại docs

e