MULTI-MASTER-PKI TUTORIAL WITH FAILOVER

- Cấu hình 1 single minion có thể có nhiều master và fail-over (chịu lỗi) nếu master đang liên kết gặp lỗi.

Các bước:

1. Setup master(s) ký chứng thực quyền chứng thực.

2. Setup minion(s) xác nhận master-public-keys.

3. Cho phép nhiều masters trên minion(s).

4. Cho phép master-check trên minion.

MOTIVATION

- Trạng thái mặc định của salt-minion là connect tới master và chấp nhận master public key. Với mỗi ban hành, master sẽ gỏi public key cho minion check xem public key của master tại minion có bị thay đổi không, minion sẽ xác nhận lại. Vì lý do này, thông thường minion chỉ được kết nối tới 1 master.

- Mục tiêu, thêm 1 số loại chứng thực đê kiểm tra khóa công khai đầu tiên minion nhận được từ master. Hiện tại, minion lấy key public master đầu tiên nhận được.

THE GOAL

- Setup master ký public key mà nó gửi tới minion, cho phép minions xác nhận chữ ký cho việc chứng thực.

PREPPING THE MASTER TO SIGN ITS PUBLIC KEY

- Để signing hoạt động, cả master và minion đều phải bật cơ chế signing hoặc xác minh.

- Nếu master ký public key nhưng minion không xác thực nó, minion sẽ không kết nối. Nếu master ko ký nhưng minion cố gắng xác thực, master cũng sẽ ko chấp nhận.

Cấu hình master ký public key của chính nó

master\_sign\_pubkey: True

- Sau khi restart salt-master service, master sẽ tự động sinh ra cặp khóa mới.

master\_sign.pem

master\_sign.pub

- custom name có thể được tùy chỉnh

master\_sign\_key\_name: <name\_without\_suffix>

- Master sẽ sinh ra 1 cập khóa mới sau khi khởi động lại và sử dụng nó để tạo ra public key mới cho việc auth-reply.

- Quá trình xử lý sẽ được thực hiện đối với mỗi yêu cầu chứng thực của minion. Nếu các minion chứng thực thường xuyên, sử dụng config\_master:master\_pubkey\_signature và conf\_master:master\_use\_pubkey\_signature setting.

- Nếu multiple master đang sử dụng và đã ký xác nhận, cặp khóa master\_sign.\* cần được copy tới mỗi master. Nếu không, minion sẽ lỗi khi xác nhận master public khi kết nối tới master khác. Vấn đề này xảy ra vì cặp khóa public được sinh ra khác nhau.

PREPPING THE MINION TO VERIFY RECEIVED PUBLIC KEYS

- Minion cần phải có public key để xác minh chữ ký nó nhận được. Public key (defaults master\_sign.pub) cần được copy từ master tới tất cả minion pki-directory.

/etc/salt/pki/minion/master\_sign.pub

DO NOT COPY THE master\_sign.pem FILE. IT MUST STAY ON THE MASTER AND

ONLY THERE!

- Sau khi copy, cho phép chữ ký kiểm tra lại minion config.

verify\_master\_pubkey\_sign: True

- Restart lại minion. Tại lần đầu tiên, có thể sử dụng chế độ debug mode để kiểm tra.

salt-minion -l debug

- Nếu connect tới master.

[DEBUG ] Attempting to authenticate with the Salt Master at 172.16.0.10

[DEBUG ] Loaded minion key: /etc/salt/pki/minion/minion.pem

[DEBUG ] salt.crypt.verify\_signature: Loading public key

[DEBUG ] salt.crypt.verify\_signature: Verifying signature

[DEBUG ] Successfully verified signature of master public key with verification public key master\_sign.pub

[INFO ] Received signed and verified master pubkey from master 172.16.0.10

[DEBUG ] Decrypting the current master AES key

- Nếu lỗi, sẽ hiển thị

[DEBUG ] Attempting to authenticate with the Salt Master at 172.16.0.10

[DEBUG ] Loaded minion key: /etc/salt/pki/minion/minion.pem

[DEBUG ] salt.crypt.verify\_signature: Loading public key

[DEBUG ] salt.crypt.verify\_signature: Verifying signature

[DEBUG ] Failed to verify signature of public key

[CRITICAL] The Salt Master server's public key did not authenticate!

- Nếu lỗi này xảy ra, kiểm tra lại pubkey (master\_sign.pub) xem khóa giữa minion và trên master có giống nhau hay ko.

- Khi việc xác minh thành công, minion có thể chạy tiền trình.

For the paranoid among us, its also possible to verify the publication whenever it is received from the master. That is, for every single auth-attempt which can be quite frequent. For example just the start of the minion will force the signature to be checked 6 times for various things like auth, mine, highstate, etc.

If that is desired, enable the setting

##

always\_verify\_signature: True

MULTIPLE MASTERS FOR A MINION

- Cấu hình nhiều master trên minion bằng việc cấu hình:

+ list of masters addresses

+ what type of master is defined

master:

- 172.16.0.10

- 172.16.0.11

- 172.16.0.12

###

master\_type: failover

- Cấu hình “master:” là list các master có sẵn cho việc kết nối.

- Khi bắt đầu cấu hình này, nó sẽ thử kết nối với các master theo thứ tự định nghĩa.

- Kết nối ngẫu nhiên theo danh sách:

master\_shuffle: True

- Master list sau khi có cấu hình này sẽ được trộn ngẫu nhiên

- Master đầu tiên sẽ chấp nhận minion

- Đối với các minion, để nó kiểm tra master liên kết định kỳ. cấu hình

master\_alive\_interval: <seconds>

- Nếu lỗi xảy ra, minion sẽ tạm thời remove master đó ra khỏi list và thử 1 master được định nghĩa (có thể list được xáo trộn nếu config trường shuffle)

TESTING THE SETUP

- Ít nhất cần phải có 2 master đạng chạy để test failover setup

- Cả 2 master cần được chạy và bật chế đố debug tại minion

salt-minion -l debug

- Minion sẽ kết nối tới master đầu tiền trong list

[DEBUG ] Attempting to authenticate with the Salt Master at 172.16.0.10

[DEBUG ] Loaded minion key: /etc/salt/pki/minion/minion.pem

[DEBUG ] salt.crypt.verify\_signature: Loading public key

[DEBUG ] salt.crypt.verify\_signature: Verifying signature

[DEBUG ] Successfully verified signature of master public key with verification public key master\_sign.pub

[INFO ] Received signed and verified master pubkey from master 172.16.0.10

[DEBUG ] Decrypting the current master AES key

- test.ping trên master minion, nó sẽ hiện các kết nối hiện tại để kiểm tra.

- Nếu thành công, tắt master đang liên kết (mẹo sử dụng firewall chặn gói tin của SaltStack)

- Dựa trên cấu hình tham số conf\_minion:master\_alive\_interval, minion sẽ thông báo kết nối lỗi và hiện thị ra logfile.

[INFO ] Connection to master 172.16.0.10 lost

[INFO ] Trying to tune in to next master from master-list

- Minion sẽ remove current master hiện tại trong list, lấy master tiếp theo cố gắng kết nối:

[INFO ] Removing possibly failed master 172.16.0.10 from list of masters

[WARNING ] Master ip address changed from 172.16.0.10 to 172.16.0.11

[DEBUG ] Attempting to authenticate with the Salt Master at 172.16.0.11

- Nếu các config chính xác, 1 master public key sẽ được xác nhận thành công

[DEBUG ] Loaded minion key: /etc/salt/pki/minion/minion.pem

[DEBUG ] salt.crypt.verify\_signature: Loading public key

[DEBUG ] salt.crypt.verify\_signature: Verifying signature

[DEBUG ] Successfully verified signature of master public key with verification public key master\_sign.pub

- authentication with the new master is successful

[INFO ] Received signed and verified master pubkey from master 172.16.0.11

[DEBUG ] Decrypting the current master AES key

[DEBUG ] Loaded minion key: /etc/salt/pki/minion/minion.pem

[INFO ] Authentication with master successful!

PERFORMANCE TUNING

e