Tìm hiểu về main config trong Puppet

- Là file cấu hình chính của Puppet.

- Sử dụng để cấu hình toàn bộ Puppet commands và services, bao gồm Puppet master, Puppet agent, Puppet apply, Puppet cert

Location

- Nằm tại: $confdir/puppet.conf

Examples

Example agent config

[main]

certname = agent01.example.com

server = puppet

environment = production

runinterval = 1h

Example master config

[main]

certname = puppetmaster01.example.com

server = puppet

environment = production

runinterval = 1h

strict\_variables = true

[master]

dns\_alt\_names = puppetmaster01,puppetmaster01.example.com,puppet,puppet.example.com

reports = puppetdb

storeconfigs\_backend = puppetdb

storeconfigs = true

environment\_timeout = unlimited

Format

- Bao gồm 1 hoặc nhiều config sections, và mỗi phần có thể 1 số settings

Config sections

[main]

certname = puppetmaster01.example.com

Config section: 1 tập các cấu hình, bao gồm

- name: được đặt trong [..], cần được đặt trong riêng 1 dòng, không được chứa khoảng trắng

- nếu xuất hiện 1 [..] khác, thì nó coi nhưng đóng lại phần config của [..] trước

Puppet sử dụng 4 config sections:

- main: cấu hình chính, sử dụng cho tất cả commands và services, có thể bị override lại bởi 1 section khác

- master: sử dụng cho puppet master và puppet cert cmd

- agent: sử dụng cho puppet client

- user: sử dụng cho puppet apply cmd

Note: nếu không tìm được section, các config sẽ tự động thuộc main sections

Bỏ qua setting config

- Bắt đầu bằng dấu #

Comment lines

# This is a comment.

Setting lines

certname = puppetmaster01.example.com

1 Setting line bao gồm:

- Bất kỳ khoảng trắng

- tên của setting

- dấu =

- giá trị được set

Một số loại giá trị đặc biệt cho setting

Lists of words:

- Chứa tập các giá trị, VD: report = http,puppetdb

Paths:

- sử dụng dấu :

# \*nix version:

environmentpath = $codedir/special\_environments:$codedir/environments

Files or directories

- 1 số loại file có thể sẽ được puppet gán thêm permission khi chạy (mặc dù có thể bỏ qua nó)

ssldir = $vardir/ssl {owner = service, mode = 0771}

Sự tùy biến trong cài đặt

- Các tùy chọn có thể thêm dấu $

ssldir = $vardir/ssl

Tìm hiểu về environment.conf trong Puppet

- Sử dụng để override lại 1 số cấu hình mặc định cơ bản của Puppet trong các môi trường khác nhau

Location

- Nằm trong $codedir/environments

- Sau đó là các file manifests và modules

Example

* VD: test environment’s config file sẽ nằm trong $codedir/environments/test/environment.conf.

# /etc/puppetlabs/code/environments/test/environment.conf

# Puppet Enterprise requires $basemodulepath; see note below under "modulepath".

modulepath = site:dist:modules:$basemodulepath

# Use our custom script to get a git commit for the current state of the code:

config\_version = get\_environment\_commit.sh

Format

- Có cấu trúc format giống với main config nhưng ko thể chưa [main] sections

- Nó không được thuộc bất kỳ config section nào

Relative paths in values

- có phép sử dụng file paths hoặc list file path

VD: Nếu tại set config\_version = get\_environment\_commit.sh trong test environment thì puppet sẽ sử dụng file /etc/puppetlabs/code/environments/test/get\_environment\_commit.sh

Interpolation in values

- có thể sử dụng giá trị từ 1 setting khác

- $environment là biến đặc biệt, cho phép lấu giá trị đường dẫn cho this environments

1 số biển hữu dựng trong environment.conf

- $basemodulepath, $environment, $codedir

Tìm hiểu về auth.conf trong Puppet

- Việc truy cập Puppet HTTPS API được cấu hình trong auth.conf

Puppet’s HTTPS API

- Puppet agent service yếu cấu các cấu hình thông qua HTTPS, puppets master cung cấp các HTTPS endpoint để support vấn đề đó, nhưng có 1 số end point không được sử dụng bởi Puppet agent

- Để giải quyết vấn đề đó, puppet sử dụng auth.config, nó chứ 1 tập các access rule cho tất cả các HTTPs service

Location

- Được lưu trữ tại $confdir/auth.conf

Example

path /puppet/v3/environments

method find

allow \*

# allow nodes to retrieve their own catalog

path ~ ^/puppet/v3/catalog/([^/]+)$

method find

allow $1

# allow nodes to retrieve their own node definition

path ~ ^/puppet/v3/node/([^/]+)$

method find

allow $1

# allow all nodes to store their own reports

path ~ ^/puppet/v3/report/([^/]+)$

method save

allow $1

# control access to the custom user\_files mount point

path ~ ^/puppet/v3/file\_(metadata|content)s?/user\_files/

auth yes

allow \*.example.com

allow\_ip 192.168.100.0/24

# allow all nodes to access all file services.

path /puppet/v3/file

allow \*

path /puppet/v3/status

method find

allow \*

# allow all nodes to access the certificates services

path /puppet-ca/v1/certificate\_revocation\_list/ca

method find

allow \*

### Unauthenticated ACLs, for clients without valid certificates; authenticated

### clients can also access these paths, though they rarely need to.

# allow access to the CA certificate; unauthenticated nodes need this

# in order to validate the puppet master's certificate

path /puppet-ca/v1/certificate/ca

auth any

method find

allow \*

# allow nodes to retrieve the certificate they requested earlier

path /puppet-ca/v1/certificate/

auth any

method find

allow \*

# allow nodes to request a new certificate

path /puppet-ca/v1/certificate\_request

auth any

method find, save

allow \*

# deny everything else; this ACL is not strictly necessary, but

# illustrates the default policy.

path /

auth any

Access control behavior

- Khi nhận được 1 HTTPs request, nó sẽ kiểm tra lại trong authorization rules, nếu thuộc rule cho phép thì sẽ chập nhận và ngược lại

- Nói đơn giản, author rule giống 1 firewall đơn giản

Default auth rules

- Puppet master có 2 tập rule: auth.conf (sẽ được kiếm tra trước), hardcode default (được kiếm tra sau)

- Không tùy chỉnh hardcode rule (vấn đề về tính nhất quán)

ACL syntax

path ~ ^/puppet/v3/report/([^/]+)$

method save

allow $1

Các thuộc tính trong 1 ACL

* path: Which URLs the ACL applies to. Required. Must be the first directive in the ACL.
* environment: Which environments the ACL applies to. Optional; defaults to all environments.
* method: Which HTTP methods the ACL applies to. Optional; defaults to all methods.
* auth: Whether the ACL applies to client-verified or non-client-verified HTTPS requests. Optional; defaults to yes (verified).
* allow: Which certificate names or hostnames can make matching requests. Optional; defaults to allowing no one.
* allow\_ip: Which IP addresses can make matching requests. Optional; defaults to allowing no one

Tìm hiểu puppetdb.conf

<https://docs.puppet.com/puppet/5.0/config_file_puppetdb.html>

Location

- Nằm tại $confdir/puppetdb.conf

Example

[main]

server = puppetdb.example.com

port = 8081

Format

* server setting must be set to the hostname of the PuppetDB server.
* port setting must be set to the port of the PuppetDB server.

Tìm hiểu autosign.conf

- Tự động chấp nhận các request mong muốn được signed. Chỉ chấp nhận trên CA Puppet master server

- Puppet master không hỗ trợ CA không sử dụng autosign.conf

Location

- Vị trí: $confdir/autosign.conf

Format:

- chứa list các cert name hoặc domain name

rebuilt.example.com

\*.scratch.example.com

\*.local

https://docs.puppet.com/puppet/5.0/config\_file\_autosign.html

Config files: device.conf

https://docs.puppet.com/puppet/5.0/config\_file\_device.html

Tìm hiểu hiera.yaml v5

<https://docs.puppet.com/puppet/5.0/hiera_config_yaml_5.html>

Config files: csr\_attributes.yaml

<https://docs.puppet.com/puppet/5.0/config_file_csr_attributes.html>

Config files: custom\_trusted\_oid\_mapping.yaml

<https://docs.puppet.com/puppet/5.0/config_file_oid_map.html>

Config files: routes.yaml

<https://docs.puppet.com/puppet/5.0/config_file_routes.html>

Configuration: Short list of important settings

<https://docs.puppet.com/puppet/5.0/config_important_settings.html>