# kolla部署——keystone配置

keystone容器中除了有部署keystone项目以为还部署了httpd，通过python的wsgi方式，将Keystone的endpiont通过httpd暴露出去，再在最外层通过haproxy和keepalived方式对httpd server做高可用。 以下是一些配置文件分解，haproxy和keepalived的讲解见《kolla部署——服务高可用》。

# wsgi-keystone.conf

Listen 192.168.102.15:5000 #public 和 internal的endpoint监听地址和端口配置

Listen 192.168.102.15:35357 #admin的endpoint监听地址和端口配置

<VirtualHost \*:5000>

WSGIDaemonProcess keystone-public processes=5 threads=1 user=keystone group=keystone display-name=%{GROUP} python-path=/var/lib/kolla/venv/lib/python2.7/site-packages #代码目录

WSGIProcessGroup keystone-public

WSGIScriptAlias / /var/www/cgi-bin/keystone/main #wsgi的启动脚本，该文件是httpd和keystone代码的桥梁

WSGIApplicationGroup %{GLOBAL}

WSGIPassAuthorization On

<IfVersion >= 2.4>

ErrorLogFormat "%{cu}t %M"

</IfVersion>

ErrorLog "/var/log/kolla/keystone/keystone-apache-public-error.log"

LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b %D \"%{Referer}i\" \"%{User-Agent}i\"" logformat #定义日志格式

CustomLog "/var/log/kolla/keystone/keystone-apache-public-access.log" logformat

</VirtualHost>

<VirtualHost \*:35357>

WSGIDaemonProcess keystone-admin processes=5 threads=1 user=keystone group=keystone display-name=%{GROUP} python-path=/var/lib/kolla/venv/lib/python2.7/site-packages

WSGIProcessGroup keystone-admin

WSGIScriptAlias / /var/www/cgi-bin/keystone/admin

WSGIApplicationGroup %{GLOBAL}

WSGIPassAuthorization On

<IfVersion >= 2.4>

ErrorLogFormat "%{cu}t %M"

</IfVersion>

ErrorLog "/var/log/kolla/keystone/keystone-apache-admin-error.log"

LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b %D \"%{Referer}i\" \"%{User-Agent}i\"" logformat

CustomLog "/var/log/kolla/keystone/keystone-apache-admin-access.log" logformat

</VirtualHost>

# Keystone.conf

## Kolla 默认配置项

[DEFAULT]

debug = False # debug模式默认关闭，如果想要调试程序，可以配置成开启，在log中看到debug信息。

log\_file = /var/log/kolla/keystone/keystone.log # 日志存放位置

use\_stderr = True #记录日志输出标准错误， 如果log\_config\_append设置了，这个配置项会被忽略。

# DEPRECATED: The HTTP Header that will be used to determine what the original

# request protocol scheme was, even if it was hidden by a SSL termination

# proxy. (string value)

# This option is deprecated for removal.

# Its value may be silently ignored in the future.

secure\_proxy\_ssl\_header = HTTP\_X\_FORWARDED\_PROTO

[database]

#配置数据库的连接，这里配置的ip是ha后的vip地址

connection = mysql+pymysql://keystone:TyiRuMS0FPjVXXdkWb9vEx6eExsOmCl9JfRXqVsF@192.168.102.47:3306/keystone

#最大重新连接次数，设置为-1表示无上限次数

max\_retries = -1

[token]

# This toggles support for revoking individual tokens by the token identifier

# and thus various token enumeration operations (such as listing all tokens

# issued to a specific user). These operations are used to determine the list

# of tokens to consider revoked. Do not disable this option if you're using the

# `kvs` `[revoke] driver`. (boolean value)

# 我的理解是根据token标识符撤销token的配置

revoke\_by\_id = False

# Entry point for the token provider in the `keystone.token.provider`

# namespace. The token provider controls the token construction, validation,

# and revocation operations. Keystone includes `fernet` and `uuid` token

# providers. `uuid` tokens must be persisted (using the backend specified in

# the `[token] driver` option), but do not require any extra configuration or

# setup. `fernet` tokens do not need to be persisted at all, but require that

# you run `keystone-manage fernet\_setup` (also see the `keystone-manage

# fernet\_rotate` command). (string value)

#token provider的入口，代码目录keystone.token.provider。“uuid”tokens必须被持久化。

provider = uuid

[cache]

#配置backend的cache模块，生产环境推荐memcache和Redis(dogpile.cache.redis)这两种。对于多线程和事件驱动的场景，推荐使用memcache with pooling（oslo\_cache.memcache\_pool）。测试环境和低线程服务器dogpile.cache.memory。

backend = oslo\_cache.memcache\_pool

#全局配置是否启动cache

enabled = True

#memcache servers的格式 “host:port”

memcache\_servers = 192.168.102.15:11211

## 其他重要配置项

参考 <https://docs.openstack.org/ocata/config-reference/identity/samples/keystone.conf.html>

admin\_token:

后置的一个admin token, 可理解为后门，存在安全风险，生产环境强烈推荐不配置。首次手动安装时候可以定义admin\_token, 可以通过他去创建keystone用户等，后续最好删除。

public\_endpoint, admin\_endpoint:

基本的keystone的endpoint配置，一般不配置，后续通过keystone命令行创建。

max\_project-tree\_depath:

最大项目深度，子项目中海油子项目，默认是5。配置的很大会影响性能。

list\_limit:

列表显示条数限制，如果keystone user list命令的列表显示，默认不配置，不受限。对于大集群可能需要配置。

strict\_password\_check:

绝对密码检查，如果设置成true，不按照密码的最大长度设置会报403错误。如果是false，密码超过最大长度会被截断。

insecure\_debug:

如果设置成了true,则会返回http response的更多信息（不管是否经过认证），这个选项开启适合于调试，但不安全。

verbose:

如果设置成为false，log级别是wanning，设置为true，log级别就变成info。这个配置选项将被remove掉了。

log\_date\_file: 日志时间格式，如 %Y-%m-%d %H:%M:%S。

log\_dir, log\_file: 日志目录，日志文件。

watch\_log\_file: 默认是false。当配置成true，如果log文件被remove掉了，会被检测到，自动产生一个新的log文件。该配置项生效的前提条件是log\_file必须得配置。

# Size of RPC connection pool. (integer value)

rpc\_conn\_pool\_size = 30

# The pool size limit for connections expiration policy (integer value)

#conn\_pool\_min\_size = 2

# A URL representing the messaging driver to use and its full configuration.

# (string value)

#transport\_url = <None>

# DEPRECATED: The messaging driver to use, defaults to rabbit. Other drivers

# include amqp and zmq. (string value)

# This option is deprecated for removal.

# Its value may be silently ignored in the future.

# Reason: Replaced by [DEFAULT]/transport\_url

#rpc\_backend = rabbit

# The default exchange under which topics are scoped. May be overridden by an

# exchange name specified in the transport\_url option. (string value)

#control\_exchange = keystone

# A list of role names which are prohibited from being an implied role. (list

# value)

#prohibited\_implied\_role = admin

[cache]

# Default TTL, in seconds, for any cached item in the dogpile.cache region.

# This applies to any cached method that doesn't have an explicit cache

# expiration time defined for it. (integer value)

#expiration\_time = 600

# Number of seconds memcached server is considered dead before it is tried

# again. (dogpile.cache.memcache and oslo\_cache.memcache\_pool backends only).

# (integer value)

#memcache\_dead\_retry = 300

# Timeout in seconds for every call to a server. (dogpile.cache.memcache and

# oslo\_cache.memcache\_pool backends only). (integer value)

#memcache\_socket\_timeout = 3

# Max total number of open connections to every memcached server.

# (oslo\_cache.memcache\_pool backend only). (integer value)

#memcache\_pool\_maxsize = 10

# Number of seconds a connection to memcached is held unused in the pool before

# it is closed. (oslo\_cache.memcache\_pool backend only). (integer value)

#memcache\_pool\_unused\_timeout = 60

# Number of seconds that an operation will wait to get a memcache client

# connection. (integer value)

#memcache\_pool\_connection\_get\_timeout = 10

[catalog]

# Absolute path to the file used for the templated catalog backend. This option

# is only used if the `[catalog] driver` is set to `templated`. (string value)

#template\_file = default\_catalog.templates

# Entry point for the catalog driver in the `keystone.catalog` namespace.

# Keystone provides a `sql` option (which supports basic CRUD operations

# through SQL), a `templated` option (which loads the catalog from a templated

# catalog file on disk), and a `endpoint\_filter.sql` option (which supports

# arbitrary service catalogs per project). (string value)

#driver = sql

# Toggle for catalog caching. This has no effect unless global caching is

# enabled. In a typical deployment, there is no reason to disable this.

# (boolean value)

#caching = true

# Time to cache catalog data (in seconds). This has no effect unless global and

# catalog caching are both enabled. Catalog data (services, endpoints, etc.)

# typically does not change frequently, and so a longer duration than the

# global default may be desirable. (integer value)

#cache\_time = <None>

# Maximum number of entities that will be returned in a catalog collection.

# There is typically no reason to set this, as it would be unusual for a

# deployment to have enough services or endpoints to exceed a reasonable limit.

# (integer value)

#list\_limit = <None>

[eventlet\_server]

#

# From keystone

#

# DEPRECATED: The IP address of the network interface for the public service to

# listen on. (string value)

# Deprecated group/name - [DEFAULT]/bind\_host

# Deprecated group/name - [DEFAULT]/public\_bind\_host

# This option is deprecated for removal since K.

# Its value may be silently ignored in the future.

# Reason: Support for running keystone under eventlet has been removed in the

# Newton release. These options remain for backwards compatibility because they

# are used for URL substitutions.

#public\_bind\_host = 0.0.0.0

# DEPRECATED: The port number for the public service to listen on. (port value)

# Minimum value: 0

# Maximum value: 65535

# Deprecated group/name - [DEFAULT]/public\_port

# This option is deprecated for removal since K.

# Its value may be silently ignored in the future.

# Reason: Support for running keystone under eventlet has been removed in the

# Newton release. These options remain for backwards compatibility because they

# are used for URL substitutions.

#public\_port = 5000

# DEPRECATED: The IP address of the network interface for the admin service to

# listen on. (string value)

# Deprecated group/name - [DEFAULT]/bind\_host

# Deprecated group/name - [DEFAULT]/admin\_bind\_host

# This option is deprecated for removal since K.

# Its value may be silently ignored in the future.

# Reason: Support for running keystone under eventlet has been removed in the

# Newton release. These options remain for backwards compatibility because they

# are used for URL substitutions.

#admin\_bind\_host = 0.0.0.0

# DEPRECATED: The port number for the admin service to listen on. (port value)

# Minimum value: 0

# Maximum value: 65535

# Deprecated group/name - [DEFAULT]/admin\_port

# This option is deprecated for removal since K.

# Its value may be silently ignored in the future.

# Reason: Support for running keystone under eventlet has been removed in the

# Newton release. These options remain for backwards compatibility because they

# are used for URL substitutions.

#admin\_port = 35357

[paste\_deploy]

#

# From keystone

#

# Name of (or absolute path to) the Paste Deploy configuration file that

# composes middleware and the keystone application itself into actual WSGI

# entry points. See http://pythonpaste.org/deploy/ for additional documentation

# on the file's format. (string value)

#config\_file = keystone-paste.ini

# keystone-paste.ini

这个文件的作用是配置了中间件和keystone应用程序本身的WSGI入口，这个文件一般不会去修改。

composes middleware and the keystone application itself into actual WSGI entry points.

[filter:debug]

use = egg:oslo.middleware#debug

[filter:request\_id]

use = egg:oslo.middleware#request\_id

[filter:build\_auth\_context]

use = egg:keystone#build\_auth\_context

[filter:token\_auth]

use = egg:keystone#token\_auth

[filter:json\_body]

use = egg:keystone#json\_body

[filter:cors]

use = egg:oslo.middleware#cors

oslo\_config\_project = keystone

[filter:ec2\_extension]

use = egg:keystone#ec2\_extension

[filter:ec2\_extension\_v3]

use = egg:keystone#ec2\_extension\_v3

[filter:s3\_extension]

use = egg:keystone#s3\_extension

[filter:url\_normalize]

use = egg:keystone#url\_normalize

[filter:sizelimit]

use = egg:oslo.middleware#sizelimit

[app:public\_service]

use = egg:keystone#public\_service

[app:service\_v3]

use = egg:keystone#service\_v3

[app:admin\_service]

use = egg:keystone#admin\_service

[pipeline:public\_api]

# The last item in this pipeline must be public\_service or an equivalent

# application. It cannot be a filter.

pipeline = cors sizelimit url\_normalize request\_id build\_auth\_context token\_auth json\_body ec2\_extension public\_service

[pipeline:admin\_api]

# The last item in this pipeline must be admin\_service or an equivalent

# application. It cannot be a filter.

pipeline = cors sizelimit url\_normalize request\_id build\_auth\_context token\_auth json\_body ec2\_extension s3\_extension admin\_service

[pipeline:api\_v3]

# The last item in this pipeline must be service\_v3 or an equivalent

# application. It cannot be a filter.

pipeline = cors sizelimit url\_normalize request\_id build\_auth\_context token\_auth json\_body ec2\_extension\_v3 s3\_extension service\_v3

[app:public\_version\_service]

use = egg:keystone#public\_version\_service

[app:admin\_version\_service]

use = egg:keystone#admin\_version\_service

[pipeline:public\_version\_api]

pipeline = cors sizelimit url\_normalize public\_version\_service

[pipeline:admin\_version\_api]

pipeline = cors sizelimit url\_normalize admin\_version\_service

[composite:main]

use = egg:Paste#urlmap

/v2.0 = public\_api

/v3 = api\_v3

/ = public\_version\_api

[composite:admin]

use = egg:Paste#urlmap

/v2.0 = admin\_api

/v3 = api\_v3

/ = admin\_version\_api