

Fetnet token local validation in multi-site scenario

1. group of docker containers to emulate two sites: Kista and Solna

```
root@docker-15:/home/ci/dockers# docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
2b34bd272b19	hafe/glance	"/bin/glance-api-sta	18 minutes ago	Up 2 minutes	9191/tcp, 9292/tcp	glance_api_Solna
32f5f5728235	hafe/glance	"/bin/glance-registr	18 minutes ago	Up 2 minutes	9191/tcp, 9292/tcp	glance_registry_Solna
27b22dab4d39	hafe/openstack-client	"/bin/bash"	34 minutes ago	Up 33 minutes		silly_kirch
97b06313e882	hafe/keystone	"/start.sh"	3 hours ago	Up 2 hours	5000/tcp, 35357/tcp	keystone_Solna
2404eba5e2aa	memcached	"memcached"	3 days ago	Up 3 days	11211/tcp	memcached_Solna
a2b6d4085f3b	hafe/mysql-galera	"/start.sh node"	3 days ago	Up 3 days	3306/tcp, 4444/tcp, 4567-4568/tcp	mysql-Solna-23
2bbd8511c168	hafe/mysql-galera	"/start.sh node"	3 days ago	Up 3 days	3306/tcp, 4444/tcp, 4567-4568/tcp	mysql-Solna-22
3dbb9eaf3a23	hafe/mysql-galera	"/start.sh master"	3 days ago	Up 3 days	3306/tcp, 4444/tcp, 4567-4568/tcp	mysql-Solna-21
ee93bf7839c8	hafe/glance	"/bin/glance-api-sta	3 days ago	Up 3 days	9191/tcp, 9292/tcp	glance_api_Kista
9438ec56032a	hafe/glance	"/bin/glance-registr	3 days ago	Up 3 days	9191/tcp, 9292/tcp	glance_registry_Kista
1f1a88a8cdc0	hafe/keystone	"/start.sh"	3 days ago	Up 3 days	5000/tcp, 35357/tcp	keystone_Kista
3432c9b51a66	memcached	"memcached"	3 days ago	Up 3 days	11211/tcp	memcached_Kista
a4d075e102ff	hafe/mysql-galera	"/start.sh node"	3 days ago	Up 3 days	3306/tcp, 4444/tcp, 4567-4568/tcp	mysql-Kista-13
74341000b083	hafe/mysql-galera	"/start.sh node"	3 days ago	Up 3 days	3306/tcp, 4444/tcp, 4567-4568/tcp	mysql-Kista-12
c86202486aa1	hafe/mysql-galera	"/start.sh master"	3 days ago	Up 3 days	3306/tcp, 4444/tcp, 4567-4568/tcp	mysql-Kista-11
fbe33901c238	dinkel/openldap	"/entrypoint.sh slap	3 days ago	Up 3 days	389/tcp	slapd

(Thanks to Hans first for the script to create the prototype environment. all these docker containers were created through the script

<https://github.com/chaovihuana/dockers>, which was forked from <https://github.com/hafe/dockers>, because the repository of hafe/dockers is updated constantly by Hans, so no gurantee that you will create same containers collection as above if you use the script mentioned in these two repository. And especially, if you want to change the configuration for KeyStone/Glance, you may have to change the script used to create the container image, and rebuild the image after modification)

Site Kista was installed with KeyStone, MySql Galera Cluster, and Glance.

Site Solna was also installed with KeyStone, MySql Galera Cluster, and Glance.

The MySql Galera Cluster in Kista is the master cluster, and the MySql Galera Cluster in Solna was configured with asynchronous replication from the Kista Cluster, only the KeyStone database will be replicated.

The token format used in the multi-site scenario is Fernet.

After a token was issued from Kista site, the token validation should be done locally and successfully if Glance api in Solna is called. Unfortunately, the token validation was redirected to Kista KeyStone, although the request was processed successfully. See issue report from

<https://docs.google.com/document/d/1pvYWQprRH3jnzX2j-zQwAErdPWg9zwkguSyLx1EBKas/edit>

The following chapter will describe how to address this issue.

2. bug in keystonemiddleware that the Keystone server can't be configured for token validation

To make the token validation can be done locally, the keystone server url could be configured or filtered.

In the prototype, I just simply use the configuration item of "auth_uri" as the keystone server for the local token validation. The source code was changed as following:

```
root@2b34bd272b19:/# find / -type d -name auth_token
/usr/lib/python2.7/dist-packages/keystonemiddleware/auth_token
/usr/lib/python2.7/dist-packages/keystonemiddleware/tests/auth_token
root@2b34bd272b19:/# vim /usr/lib/python2.7/dist-packages/keystonemiddleware/auth_token/__init__.py

class AuthProtocol(object):
    """Middleware that handles authenticating client calls."""

    def __init__(self, app, conf):
        # .....

        # get configuration _auth_uri before calling _create_identity_server
        self._auth_uri = self._conf_get('auth_uri')
        self._identity_server = self._create_identity_server()

        # self._auth_uri = self._conf_get('auth_uri')
        if not self._auth_uri:
            self._LOG.warning(
                _LW('Configuring auth_uri to point to the public identity '
                    'endpoint is required; clients may not be able to '
                    'authenticate against an admin endpoint'))

    def _create_identity_server(self):
        sess = session.Session.construct(dict(
            cert=self._conf_get('certfile'),
            key=self._conf_get('keyfile'),
            cacert=self._conf_get('cafile'),
            insecure=self._conf_get('insecure'),
            timeout=self._conf_get('http_connect_timeout')
        ))

        auth_plugin = self._get_auth_plugin()

        #pass the authentication uri to the adapter, so that the Keystone client understand that the configured authentication server (Keystone ) address
        #should be used instead for the token validation.
        endpoint_conf = None
        if self._auth_uri:
            endpoint_conf = self._auth_uri

        adap = adapter.Adapter(
            sess,
            auth=auth_plugin,
            service_type='identity',
            interface='admin',
            endpoint_override=endpoint_conf,
```

```
connect_retries=self._conf_get('http_request_max_retries'))
```

3. add some trace code to verify the modification

The token validation request will be forwarded to the KeyStone server by the KeyStoneClient. Add some code to trace the request.

```
root@2b34bd272b19:/# find / -type d -name keystoneclient
/usr/lib/python2.7/dist-packages/keystoneclient
root@2b34bd272b19:/# vim /usr/lib/python2.7/dist-packages/keystoneclient/session.py
```

```
@utils.positional(enforcement=utils.positional.WARN)
def request(self, url, method, json=None, original_ip=None,
            user_agent=None, redirect=None, authenticated=None,
            endpoint_filter=None, auth=None, requests_auth=None,
            raise_exc=True, allow_reauth=True, log=True,
            endpoint_override=None, connect_retries=0, **kwargs):

    if log:
        self._http_log_request(url, method=method,
                               data=kwargs.get('data'),
                               headers=headers)

    # Force disable requests redirect handling. We will manage this below.
    kwargs['allow_redirects'] = False

    if redirect is None:
        redirect = self.redirect

    send = functools.partial(self._send_request,
                              url, method, redirect, log, connect_retries)
    resp = send(**kwargs)if not urllib.parse.urlparse(url).netloc:
        base_url = None

    if endpoint_override:
        base_url = endpoint_override
        _logger.debug('#####1: base_url = %s', base_url )
    elif endpoint_filter:
        base_url = self.get_endpoint(auth, **endpoint_filter)
        _logger.debug('#####2: base_url = %s', base_url )

    if not base_url:
        raise exceptions.EndpointNotFound()

    url = '%s/%s' % (base_url.rstrip('/'), url.lstrip('/'))
    _logger.debug('#####3: url = %s', url )

    if self.cert:
        kwargs.setdefault('cert', self.cert)

    if self.timeout is not None:
        kwargs.setdefault('timeout', self.timeout)
```

```

if user_agent:
    headers['User-Agent'] = user_agent
elif self.user_agent:
    user_agent = headers.setdefault('User-Agent', self.user_agent)
else:
    user_agent = headers.setdefault('User-Agent', USER_AGENT)

if self.original_ip:
    headers.setdefault('Forwarded',
        'for=%s;by=%s' % (self.original_ip, user_agent))

if json is not None:
    headers['Content-Type'] = 'application/json'
    kwargs['data'] = jsonutils.dumps(json)

kwargs.setdefault('verify', self.verify)

if requests_auth:
    kwargs['auth'] = requests_auth

_logger.debug('#####4: url = %s, method = %s, headers = %s', url, method, headers )

```

4. Check the address of Solna KeyStone

```

root@docker-15:/home/ci/dockers# docker exec -it 97b06313e882 bash
root@97b06313e882:/# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
204: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:62 brd ff:ff:ff:ff:ff:ff
    #Solna KeyStone server IP address
    inet 172.17.0.98/16 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:acff:fe11:62/64 scope link
        valid_lft forever preferred_lft forever

```

5. Configure the Glance in Solna

The token validation request will be forwarded to the KeyStone server by the KeyStoneClient. Add some code to trace the request.

```

root@docker-15:/home/ci/dockers# docker exec -it 2b34bd272b19 bash
root@2b34bd272b19:/# vim etc/glance/glance-api.conf

[DEFAULT]
# Show more verbose log output (sets INFO log level output)
#verbose = False

# Show debugging output in logs (sets DEBUG log level output)

```

```
#debug = False

# Maximum image size (in bytes) that may be uploaded through the
# Glance API server. Defaults to 1 TB.
# WARNING: this value should only be increased after careful consideration
# and must be set to a value under 8 EB (9223372036854775808).
#image_size_cap = 1099511627776

# Address to bind the API server
bind_host = 0.0.0.0

# Port the bind the API server to
bind_port = 9292

# Log to this file. Make sure you do not set the same log file for both the API
# and registry servers!
#

# the container image missing this configuration, add the log configuration
# If 'log_file' is omitted and 'use_syslog' is false, then log messages are
# sent to stdout as a fallback.
log_file = /var/log/glance/glance_api.log

[keystone_authtoken]
identity_uri = http://172.17.0.98:35357
admin_tenant_name = service
admin_user = glance
admin_password = glance
revocation_cache_time = 10
auth_plugin = password
project_domain_id = default
user_domain_id = default
project_name = service
username = glance

#it's very important to configure the auth_uri with /v3, even if you configure the auth_version = 3 (some bug here?)
#http://172.17.0.98:35357 is the Solna KeyStone server address
auth_uri = http://172.17.0.98:35357/v3
auth_url = http://172.17.0.98:35357
auth_version = 3
password = glance
auth_host = 172.17.0.98
```

6. Now the token will be validated as expected locally

```
root@27b22dab4d39:~# openstack endpoint list
```

ID	Region	Service Name	Service Type	Enabled	Interface	URL
18389f1ff42640cf905351a7f9b8a6f7	Kista	glance	image	True	internal	http://172.17.0.41:9292
3bd662e362e24f45a9db2b77ad0682bb	Solna	glance	image	True	internal	http://172.17.0.116:9292
425b14d499264aa1bad8170a99afce88	Kista	keystone	identity	True	admin	http://172.17.0.36:35357
60a02a99078642d0974843323bbb8836	Solna	glance	image	True	public	http://172.17.0.116:9292
712d42d06ade4fedb8820e6f6ed33574	Kista	glance	image	True	public	http://172.17.0.41:9292
8000a62a8406437dad4759960bad837f	Kista	keystone	identity	True	public	http://172.17.0.36:5000
a7ec590712364e9f876f0b82d1879a99	Kista	keystone	identity	True	internal	http://172.17.0.36:5000

```
| bf9d05de9be64f5bb886959eb6bb367d | Solna | glance | image | True | admin | http://172.17.0.116:9292 |
| d1cb2f7d7d594199909b14a0004f37fe | Kista | glance | image | True | admin | http://172.17.0.41:9292 |
+-----+-----+-----+-----+-----+-----+-----+
```

issue token from Kista keystone.

```
root@27b22dab4d39:~# openstack token issue
```

```
+-----+-----+-----+-----+-----+-----+-----+
| Field | Value |
+-----+-----+-----+-----+-----+-----+-----+
| expires | 2015-08-21T08:07:29.471795Z |
| id | gAAAAABV1s4yL2-clHEY8Pfv4kqmXOHuuwcfMaKsObo8fJxl8jKploJTdIH1gYeTzyAZSzfZkKZwUfK78ULK5eWYhqEUJCAQpeZS1RKCS6sdXmJiMeeb-D6Fj6D9beDOKEgnZXjQMdsr01h2vF5lqqeuKhnRNiY-oAj0IA79jGp0-1rkqN11s%3D |
| project_id | 79185427679a44019d919ce34112c971 |
| user_id | 3c94437bbd0a455d938ed1d95c7049d1 |
+-----+-----+-----+-----+-----+-----+-----+
```

use the token to access Solna Glance.

```
root@27b22dab4d39:~# glance --os-auth-token
```

```
gAAAAABV1s4yL2-clHEY8Pfv4kqmXOHuuwcfMaKsObo8fJxl8jKploJTdIH1gYeTzyAZSzfZkKZwUfK78ULK5eWYhqEUJCAQpeZS1RKCS6sdXmJiMeeb-D6Fj6D9beDOKEgnZXjQMdsr01h2vF5lqqeuKhnRNiY-oAj0IA79jGp0-1rkqN11s%3D --os-image-url http://172.17.0.116:9292 image-list
```

```
+-----+-----+-----+-----+-----+
| ID | Name | Disk Format | Container Format | Size | Status |
+-----+-----+-----+-----+-----+
| a10756cc-89e6-4a62-a5d5-9e28e2384f17 | | | | | queued |
| 8cbc7cbd-1f56-4251-9d9c-3e2b59b28523 | | | | | queued |
| 9fe5545c-01cd-478a-9683-23141d9b2c5b | | | | | queued |
| 2f8453cb-be6b-4c6c-a0f3-af0401149bc0 | | | | | queued |
| 3d35ee47-ff7d-4036-bec0-446583eecd | | | | | queued |
+-----+-----+-----+-----+-----+
```

Check the request trace

```
root@2b34bd272b19:~# cat var/log/glance/glance_api.log
```

```
2015-08-21 07:39:09.039 190 DEBUG glance.api.middleware.version_negotiation [-] Determining version of request: GET /v1/images/detail Accept: */*
process_request /usr/lib/python2.7/dist-packages/glance/api/middleware/version_negotiation.py:47
2015-08-21 07:39:09.040 190 DEBUG glance.api.middleware.version_negotiation [-] Using url versioning process_request
/usr/lib/python2.7/dist-packages/glance/api/middleware/version_negotiation.py:60
2015-08-21 07:39:09.040 190 DEBUG glance.api.middleware.version_negotiation [-] Matched version: v1 process_request
/usr/lib/python2.7/dist-packages/glance/api/middleware/version_negotiation.py:72
2015-08-21 07:39:09.041 190 DEBUG glance.api.middleware.version_negotiation [-] new path /v1/images/detail process_request
/usr/lib/python2.7/dist-packages/glance/api/middleware/version_negotiation.py:73
2015-08-21 07:39:09.043 190 DEBUG keystoneclient.session [-] #####4: url = http://172.17.0.98:35357, method = GET, headers = {'Accept':
'application/json', 'User-Agent': 'python-keystoneclient'} request /usr/lib/python2.7/dist-packages/keystoneclient/session.py:364
2015-08-21 07:39:09.043 190 DEBUG keystoneclient.session [-] REQ: curl -g -i -X GET http://172.17.0.98:35357 -H "Accept: application/json" -H
"User-Agent: python-keystoneclient" _http_log_request /usr/lib/python2.7/dist-packages/keystoneclient/session.py:195
2015-08-21 07:39:09.066 190 DEBUG keystoneclient.session [-] RESP: [300] content-length: 593 vary: X-Auth-Token connection: keep-alive date: Fri, 21
Aug 2015 07:39:09 GMT content-type: application/json x-distribution: Ubuntu
RESP BODY: {"versions": {"values": [{"status": "stable", "updated": "2015-03-30T00:00:00Z", "media-types": [{"base": "application/json", "type":
"application/vnd.openstack.identity-v3+json"}], "id": "v3.4", "links": [{"href": "http://172.17.0.98:35357/v3/", "rel": "self"}]}, {"status": "stable", "updated":
"2014-04-17T00:00:00Z", "media-types": [{"base": "application/json", "type": "application/vnd.openstack.identity-v2.0+json"}], "id": "v2.0", "links": [{"href":
"http://172.17.0.98:35357/v2.0/", "rel": "self"}, {"href": "http://docs.openstack.org/", "type": "text/html", "rel": "describedby"}]}]}
_http_log_response /usr/lib/python2.7/dist-packages/keystoneclient/session.py:223
2015-08-21 07:39:09.066 190 DEBUG keystoneclient.auth.identity.v3 [-] Making authentication request to http://172.17.0.98:35357/v3/auth/tokens
get_auth_ref /usr/lib/python2.7/dist-packages/keystoneclient/auth/identity/v3.py:125
```

```
2015-08-21 07:39:09.068 190 DEBUG keystoneclient.session [-] #####4: url = http://172.17.0.98:35357/v3/auth/tokens, method = POST, headers =
{'Content-Type': 'application/json', 'Accept': 'application/json', 'User-Agent': 'python-keystoneclient'} request
/usr/lib/python2.7/dist-packages/keystoneclient/session.py:364
2015-08-21 07:39:09.198 190 DEBUG keystoneclient.session [-] #####1: base_url = http://172.17.0.98:35357/v3 request
/usr/lib/python2.7/dist-packages/keystoneclient/session.py:327
2015-08-21 07:39:09.199 190 DEBUG keystoneclient.session [-] #####3: url = http://172.17.0.98:35357/v3/auth/tokens request
/usr/lib/python2.7/dist-packages/keystoneclient/session.py:336
2015-08-21 07:39:09.199 190 DEBUG keystoneclient.session [-] #####4: url = http://172.17.0.98:35357/v3/auth/tokens, method = GET, headers =
{'X-Subject-Token':
'gAAAAABV1s4yl2-clHEY8Pfv4kqmXOHuucfdMaKsObo8fJxl8jKploJTDIHl1gYeTzyAZSzFzKkZwUfK78ULK5eWYhqEUJCAQpeZS1RKCS6sdXmJiMeeb-
D6Fj6D9beDOKEgnZXjQMdsr01h2vF5lqqeuKhnrNIY-oAj0IA79jGp0-1rkqN11s%3D', 'User-Agent': 'python-keystoneclient', 'Accept': 'application/json',
'X-Auth-Token':
'gAAAAABV1tWd03h4wgP2xDdkcTq3nJBI3oOyl3f2BPANh1xHr8HEI3FId-Xkh8l_SYkV3YxredZnwHfH1hJM4V2uMbl-4VXe6TMV2afKY8WbscKOVuXDoLwEa
Rc5z-0GNROxqFwIWt9Y8TMNKTgyqj3MfZ20zOqLm8bkkVmZgGc_uEO86LnOX4%3D'} request
/usr/lib/python2.7/dist-packages/keystoneclient/session.py:364
2015-08-21 07:39:09.200 190 DEBUG keystoneclient.session [-] REQ: curl -g -i -X GET http://172.17.0.98:35357/v3/auth/tokens -H "X-Subject-Token:
{SHA1}f8ef1238f960957325cc102ece011faba8b3fc67" -H "User-Agent: python-keystoneclient" -H "Accept: application/json" -H "X-Auth-Token:
{SHA1}a8273d901451dd7cea4256f2cee8f0550ab17f38" _http_log_request /usr/lib/python2.7/dist-packages/keystoneclient/session.py:195
2015-08-21 07:39:09.429 190 DEBUG keystoneclient.session [-] RESP: [200] content-length: 1980 x-subject-token:
{SHA1}f8ef1238f960957325cc102ece011faba8b3fc67 vary: X-Auth-Token x-distribution: Ubuntu connection: keep-alive date: Fri, 21 Aug 2015 07:39:09
GMT content-type: application/json x-openstack-request-id: req-212f2a74-68d3-4062-b4f6-103c168d8676
RESP BODY: {"token": {"methods": ["password"], "roles": [{"id": "a4935779c40f45d3ba7a8eeada0f7714", "name": "admin"}], "expires_at":
"2015-08-21T08:07:29.000000Z", "project": {"domain": {"id": "default", "name": "Default"}, "id": "79185427679a44019d919ce34112c971", "name": "admin"},
"catalog": "<removed>", "extras": {}, "user": {"domain": {"id": "default", "name": "Default"}, "id": "3c94437bbd0a455d938ed1d95c7049d1", "name": "osadmin"},
"audit_ids": ["nNdY2mb9SseEhcfZSIW4Ow"]}, "issued_at": "2015-08-21T07:07:30.000000Z"}}
_http_log_response /usr/lib/python2.7/dist-packages/keystoneclient/session.py:223
2015-08-21 07:39:09.436 190 DEBUG oslo_policy.openstack.common.fileutils [req-3c21c6b8-7ea3-41b9-89d7-0cd11f5641c5
3c94437bbd0a455d938ed1d95c7049d1 79185427679a44019d919ce34112c971 - - -] Reloading cached file /etc/glance/policy.json read_cached_file
/usr/lib/python2.7/dist-packages/oslo_policy/openstack/common/fileutils.py:64
2015-08-21 07:39:09.444 190 DEBUG oslo_policy.policy [req-3c21c6b8-7ea3-41b9-89d7-0cd11f5641c5 3c94437bbd0a455d938ed1d95c7049d1
79185427679a44019d919ce34112c971 - - -] Reloaded policy file: /etc/glance/policy.json _load_policy_file
/usr/lib/python2.7/dist-packages/oslo_policy/policy.py:403
2015-08-21 07:39:09.448 190 DEBUG glance.common.client [req-3c21c6b8-7ea3-41b9-89d7-0cd11f5641c5 3c94437bbd0a455d938ed1d95c7049d1
79185427679a44019d919ce34112c971 - - -] Constructed URL: http://172.17.0.115:9191/images/detail?sort_key=name&sort_dir=asc&limit=20
_construct_url /usr/lib/python2.7/dist-packages/glance/common/client.py:401
2015-08-21 07:39:09.891 190 DEBUG glance.registry.client.v1.client [req-3c21c6b8-7ea3-41b9-89d7-0cd11f5641c5 3c94437bbd0a455d938ed1d95c7049d1
79185427679a44019d919ce34112c971 - - -] Registry request GET /images/detail HTTP 200 request id req-req-4bbe2d45-b2d7-4871-a6af-ff57808414e0
do_request /usr/lib/python2.7/dist-packages/glance/registry/client/v1/client.py:124
2015-08-21 07:39:09.893 190 INFO eventlet.wsgi.server [req-3c21c6b8-7ea3-41b9-89d7-0cd11f5641c5 3c94437bbd0a455d938ed1d95c7049d1
79185427679a44019d919ce34112c971 - - -] 172.17.0.108 - - [21/Aug/2015 07:39:09] "GET /v1/images/detail?sort_key=name&sort_dir=asc&limit=20
HTTP/1.1" 200 2421 0.856376
```