

Test su Vault & htgettoken trilaterale 25-11-21

User Support group

Configurazione high availability con HAproxy

- **Macchine a disposizione:**

- 3 server vault:

- vm-131-154-161-16.cr.cnaf.infn.it;
 - vm-131-154-161-31.cr.cnaf.infn.it;
 - vm-131-154-161-130.cr.cnaf.infn.it

- Vm con Haproxy:

- vm-131-154-161-107.cr.cnaf.infn.it

- Viene editato il file di configurazione `parameters.yaml`, indicando nome del cluster, nome della vm master, peer1 e peer2.

```
cluster:  
  name: vm-131-154-161-107.cr.cnaf.infn.it  
  master: vm-131-154-161-16.cr.cnaf.infn.it  
  peer1: vm-131-154-161-130.cr.cnaf.infn.it  
  peer2: vm-131-154-161-31.cr.cnaf.infn.it  
[root@vm-131-154-161-16 ~]#
```

Configurazione high availability con HAproxy

● Configurazione Kerberos auth:

- Editato il parameters.yaml
- Aggiunto keytab sulla master vm

```
kerberos:  
  - name: cnaf  
    ldapurl: ldap://ldap-m.cr.cnaf.infn.it  
    ldapdn: ou=people,ou=cnaf,o=infn,c=it  
    ldapattr: uid  
    policydomain: cr.cnaf.infn.it
```

```
[root@vm-131-154-161-16 ~]# klist -k /etc/krb5-cnaf.keytab  
Keytab name: FILE:/etc/krb5-cnaf.keytab  
KVNO Principal  
-----  
   3 host/vm-131-154-161-107.cr.cnaf.infn.it@CR.CNAF.INFN.IT  
   3 host/vm-131-154-161-107.cr.cnaf.infn.it@CR.CNAF.INFN.IT  
[root@vm-131-154-161-16 ~]#  
[root@vm-131-154-161-16 ~]# █
```

Configurazione high availability con HAproxy

- Stato del cluster

```
[root@vm-131-154-161-16 ~]# vault status
Key          Value
---          -
Seal Type    shamir
Initialized  true
Sealed       false
Total Shares 1
Threshold    1
Version      1.7.3
Storage Type raft
Cluster Name vault-cluster-5095917d
Cluster ID   e24f7539-ac00-68a1-805d-7de68c42bf09
HA Enabled   true
HA Cluster   https://vm-131-154-161-16.cr.cnaf.infn.it:8201
HA Mode      active
Active Since 2021-07-18T15:32:13.821283526Z
Raft Committed Index 126
Raft Applied Index  126
[root@vm-131-154-161-16 ~]# vault operator raft list-peers
Node          Address          State      Voter
-----
vm-131-154-161-16.cr.cnaf.infn.it  vm-131-154-161-16.cr.cnaf.infn.it:8201  leader    true
vm-131-154-161-130.cr.cnaf.infn.it  vm-131-154-161-130.cr.cnaf.infn.it:8201  follower  true
vm-131-154-161-31.cr.cnaf.infn.it   vm-131-154-161-31.cr.cnaf.infn.it:8201  follower  true
[root@vm-131-154-161-16 ~]#
```

Configurazione high availability con HAproxy

- File di configurazione HAproxy

```
#-----  
# main frontend which proxys to the backends  
#-----  
frontend htvault  
    bind 10.10.0.31:8200 ssl no-sslv3 crt /etc/security/hostcombined.pem  
    default_backend htvault  
    option tcpka  
    option tcplog
```

```
backend htvault  
    balance source  
    http-request set-header X-Forwarded-Host %[req.hdr(host)]  
    http-request set-header X-Forwarded-Port %[dst_port]  
    option tcpka  
    # option httpchk OPTIONS / HTTP/1.0\r\nUser-Agent:\ HAProxy  
    option tcplog  
    option forwardfor  
    server vm-131-154-161-16.cr.cnaf.infn.it 131.154.161.16:8200 check check-ssl inter 2000 rise 2 fall 5 ssl ca-file /etc/ssl/certs/ca-bundle.crt  
    server vm-131-154-161-31.cr.cnaf.infn.it 131.154.161.31:8200 check check-ssl inter 2000 rise 2 fall 5 ssl ca-file /etc/ssl/certs/ca-bundle.crt  
    server vm-131-154-161-130.cr.cnaf.infn.it 131.154.161.130:8200 check check-ssl inter 2000 rise 2 fall 5 ssl ca-file /etc/ssl/certs/ca-bundle.crt
```

Configurazione high availability con HAproxy

- Richiesta bearer token tramite htgettoken

```
[dlattanzio@us-ops ~]$ htgettoken -v -a vm-131-154-161-107.cr.cnaf.infn.it
Attempting OIDC authentication with https://vm-131-154-161-107.cr.cnaf.infn.it:8200

Complete the authentication via web browser at:
  https://iam-t1-computing.cloud.cnaf.infn.it/device?user\_code=WRCR00
No web open command defined, please open URL manually
Waiting for response in web browser
Storing vault token in /tmp/vt_u10164
Saving credkey to /home/USER-SUPPORT/dlattanzio/.config/htgettoken/credkey-default-default: dlattanzio
Saving refresh token to https://vm-131-154-161-107.cr.cnaf.infn.it:8200
  at path secret/oauth-default/creds/dlattanzio:default
Getting bearer token from https://vm-131-154-161-107.cr.cnaf.infn.it:8200
  at path secret/oauth-default/creds/dlattanzio:default
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$
```

Configurazione high availability con HAproxy

- Richiesta nuovo vault token tramite kerberos

- L'utente ottiene ticket kerberos con kinit:

```
[dlattanzio@us-ops ~]$ kinit -V dlattanzio
Using existing cache: persistent:10164:krb_ccache_uKYF473
Using principal: dlattanzio@CR.CNAF.INFN.IT
Password for dlattanzio@CR.CNAF.INFN.IT:
Authenticated to Kerberos v5
[dlattanzio@us-ops ~]$
```

- Lanciare htgettoken per ottenere con successo un nuovo vault token via kerberos:

```
[dlattanzio@us-ops ~]$ htgettoken -v -a vm-131-154-161-107.cr.cnaf.infn.it
Credkey from /home/USER-SUPPORT/dlattanzio/.config/htgettoken/credkey-default-default: dlattanzio
Initializing kerberos client for host@vm-131-154-161-107.cr.cnaf.infn.it
Negotiating kerberos with https://vm-131-154-161-107.cr.cnaf.infn.it:8200
  at path auth/kerberos-default_default/login
Storing vault token in /tmp/vt_u10164
Attempting to get bearer token from https://vm-131-154-161-107.cr.cnaf.infn.it:8200
  at path secret/oauth-default/creds/dlattanzio:default
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$ █
```