

Aggiornamento test su Vault & htgettoken – trilaterale 22-07-21

User Support group

Impostare un hostname di default

- Esportare l'hostname come variabile d'ambiente

```
[dlattanzio@us-ops ~]$ export HTGETTOKENOPTS="-a vm-131-154-161-16.cr.cnaf.infn.it"
[dlattanzio@us-ops ~]$
[dlattanzio@us-ops ~]$ htgettoken -v
Credkey from /home/USER-SUPPORT/dlattanzio/.config/htgettoken/credkey-default-default: dlattanzio
Attempting to get bearer token from https://vm-131-154-161-16.cr.cnaf.infn.it:8200
  using vault token from /tmp/vt_u10164
  at path secret/oauth-default/creds/dlattanzio:default
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$
[dlattanzio@us-ops ~]$ htgettoken -i default
Attempting to get token from https://vm-131-154-161-16.cr.cnaf.infn.it:8200 ... succeeded
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$
```

Riduzione degli scopes

- Nel file di configurazione ci sarà un ruolo chiamato "default" che è quello che htgettoken userà se nessun ruolo viene specificato e che contiene tutti gli scopes del client registrato su su iam.
- Poi è possibile definire dei ruoli che contengono un sottoinsieme degli scopes totali, es:

```
roles:  
  - name: default  
    scopes: [openid,profile,email,address,phone,offline_access]  
  - name: reduced  
    scopes: [openid,profile,email,offline_access]
```

Riduzione degli scopes

```
[dlattanzio@us-ops ~]$ htgettoken -v -a vm-131-154-161-16.cr.cnaf.infn.it -r reduced
Attempting OIDC authentication with https://vm-131-154-161-16.cr.cnaf.infn.it:8200

Complete the authentication via web browser at:
  https://iam-t1-computing.cloud.cnaf.infn.it/device?user_code=KUI1PV

Couldn't open browser with 'xdg-open', please open URL manually

Storing vault token in /tmp/vt_u10164
Saving credkey to /home/USER-SUPPORT/dlattanzio/.config/htgettoken/credkey-default-reduced: dlattanzio
Saving refresh token to https://vm-131-154-161-16.cr.cnaf.infn.it:8200
  at path secret/oauth-default/creds/dlattanzio:reduced
Getting bearer token from https://vm-131-154-161-16.cr.cnaf.infn.it:8200
  at path secret/oauth-default/creds/dlattanzio:reduced
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$
```

Client

Token Information

vault-test

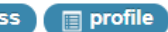
eyJraWQiOiJyc2ExIiwiaWxnIjo ...

 address  phone  openid  email  offline_access  profile

+ Refresh

vault-test

eyJraWQiOiJyc2ExIiwiaWxnIjo ...

 openid  email  offline_access  profile

+ Refresh

Limitazione durata vault token

```
[root@vm-131-154-161-16 ~]# vault write sys/auth/token/tune max_lease_ttl=24h
```

```
[root@vm-131-154-161-16 ~]# vault read sys/auth/token/tune
```

Key	Value
-----	-------

---	-----
-----	-------

default_lease_ttl	24h
-------------------	------------

description	token based credentials
-------------	-------------------------

force_no_cache	false
----------------	-------

max_lease_ttl	24h
---------------	------------

token_type	default-service
------------	-----------------

Limitazione durata vault token

- In questo modo abbiamo limitato lato server la durata massima del vault token a 24h. Se un utente proverà con htgettoken a richiederne uno di 48h, ne otterrà comunque uno di 24.

```
[dlattanzio@us-ops ~]$ htgettoken -v -a vm-131-154-161-16.cr.cnaf.infn.it --vaulttokenttl=48h
```

```
Credkey from /home/USER-SUPPORT/dlattanzio/.config/htgettoken/credkey-default-default: dlattanzio
```

```
Initializing kerberos client for host@vm-131-154-161-16.cr.cnaf.infn.it
```

```
Negotiating kerberos with https://vm-131-154-161-16.cr.cnaf.infn.it:8200
```

```
Storing vault token in /tmp/vt_u10164
```

```
[...]
```

Limitazione durata vault token

- In questo modo abbiamo limitato lato server la durata massima del vault token a 24h. Se un utente proverà con `htgettoken` a richiederne uno di 48h, ne otterrà comunque uno di 24.

```
[root@vm-131-154-161-16 ~]# vault token lookup s.MCUUxmPdvoLs9Qe7A0M4bvot
```

Key	Value
---	----
accessor	MmkRGh5JOsRnZLEsWpdfmCiO
creation_time	1626374766
creation_ttl	24h

[...]

Configurazione in HA con 3 vm

- Aggiungere nel file di configurazione i parametri relativi al nome del cluster, master vm, peer1 e peer2

```
cluster:  
  name: vault-test.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
```

vm-131-154-161-16.cr.cnaf.infn.it

```
cluster:  
  name: vault-test.cr.cnaf.infn.it  
  master: vm-131-154-161-16.cr.cnaf.infn.it  
  peer1: vm-131-154-161-16.cr.cnaf.infn.it  
  peer2: vm-131-154-161-130.cr.cnaf.infn.it
```

vm-131-154-161-31.cr.cnaf.infn.it

```
cluster:  
  name: vault-test.cr.cnaf.infn.it  
  master: vm-131-154-161-16.cr.cnaf.infn.it  
  peer1: vm-131-154-161-16.cr.cnaf.infn.it  
  peer2: vm-131-154-161-31.cr.cnaf.infn.it
```

vm-131-154-161-130.cr.cnaf.infn.it

Configurazione in HA con 3 vm

- Da vault è possibile vedere in elenco quale vm è leader e chi sono le followers:

```
[root@vm-131-154-161-16 ~]# export VAULT_ADDR=http://localhost:8202
[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-131-154-161-31.cr.cnaf.infn.it	vm-131-154-161-31.cr.cnaf.infn.it:8201	follower	true
vm-131-154-161-130.cr.cnaf.infn.it	vm-131-154-161-130.cr.cnaf.infn.it:8201	follower	true

```
[root@vm-131-154-161-16 ~]#
```

- Eseguendo il restart per esempio della vm-131-154-161-16.cr.cnaf.infn.it il ruolo di leader passa ad un'altra delle due vm.

Configurazione in HA con 3 vm

```
[dlattanzio@us-ops ~]$ htgettoken -a vault-test.cr.cnaf.infn.it
Attempting OIDC authentication with https://vault-test.cr.cnaf.infn.it:8200

Complete the authentication via web browser at:
  https://iam-t1-computing.cloud.cnaf.infn.it/device?user_code=ALN1JD

Couldn't open browser with 'xdg-open', please open URL manually

Storing vault token in /tmp/vt_u10164
Saving credkey to /home/USER-SUPPORT/dlattanzio/.config/htgettoken/credkey-default-default
Saving refresh token ... done
Attempting to get token from https://vault-test.cr.cnaf.infn.it:8200 ... succeeded
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$
```

```
[dlattanzio@us-ops ~]$ htgettoken -a vm-131-154-161-16.cr.cnaf.infn.it
Attempting to get token from https://vm-131-154-161-16.cr.cnaf.infn.it:8200 ... succeeded
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$
[dlattanzio@us-ops ~]$ htgettoken -a vm-131-154-161-31.cr.cnaf.infn.it
Attempting to get token from https://vm-131-154-161-31.cr.cnaf.infn.it:8200 ... succeeded
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$
[dlattanzio@us-ops ~]$ htgettoken -a vm-131-154-161-130.cr.cnaf.infn.it
Attempting to get token from https://vm-131-154-161-130.cr.cnaf.infn.it:8200 ... succeeded
Storing bearer token in /run/user/10164/bt_u10164
[dlattanzio@us-ops ~]$ █
```

Configurazione in HA con 3 vm – NOTA:

- Stoppando la vm-131-154-161-16:

```
[dlattanzio@us-ops ~]$ htgettoken -v -a vault-test.cr.cnaf.infn.it
Attempting OIDC authentication with https://vault-test.cr.cnaf.infn.it:8200

Complete the authentication via web browser at:
https://iam-t1-computing.cloud.cnaf.infn.it/device?user_code=XP2UB1

Couldn't open browser with 'xdg-open', please open URL manually

htgettoken: Authentication to https://vault-test.cr.cnaf.infn.it:8200 failed: URLError: <urlopen error [Errno 113] No route to host>
[dlattanzio@us-ops ~]$
[dlattanzio@us-ops ~]$
[dlattanzio@us-ops ~]$ htgettoken -v -a vm-131-154-161-130.cr.cnaf.infn.it
Attempting OIDC authentication with https://vm-131-154-161-130.cr.cnaf.infn.it:8200

Complete the authentication via web browser at:
https://iam-t1-computing.cloud.cnaf.infn.it/device?user_code=RI0N27

Couldn't open browser with 'xdg-open', please open URL manually

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-131-154-161-130.cr.cnaf.infn.it:8200
  at path secret/oauth-default/creds/dlattanzio:default
Getting bearer token from https://vm-131-154-161-130.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 ~]$
```