



Dettagli sul Sistema AAI

Daniele Spiga spiga@inf.n.it



eosc-hub.eu



@EOSC_eu

Dissemination level: Public/Confidential *If confidential, please define:*

Disclosing Party: (those disclosing confidential information)

Recipient Party: (to whom this information is disclosed, default: project consortium)



Because it is a pillar

1. we discussed this on Monday while we summarized the AMS experiences and all the tested scenarios
 - a. which imply authN/Z
2. we used AAI on Tuesday. Do you remember the “dodas-iam registration issue :(“
 - a. but it recovered :) .. it was just my fault
3. we used AAI several time yesterday
 - a. sometime we were aware.. sometime not.
 - b. see later
4. and again, we need AAI.. it is a pillar generally speaking

We used Tokens and certificates X509, more than what we realized.. actually

- well we didn't see X509, but we used it
 - DN was used to configure condor_mapfile
 - X509 was needed to submit jobs from remote
- Token was used to configure TOSCA template
 - that token has been used to
 - AuthN/Z with PaaS layer
 - AuthN/Z with IaaS
 - and manage legacy (HTCondor & GSI)

(Question: why both? isn't it two times the same thing? do I need both?)

Deploy

After using the `$HOME/get_proxy.sh` script to retrieve the token, export it into an env variable together with the orchestrator endpoint:

```
export ORCHENT_TOKEN=<your token here>
```

Branch: **master** ▾ [HandsOn-INFN-2019](#) / [htc_helm](#) / [templates](#) / [tts.yaml](#) Find file Copy path

 **dciangot** Merge commit '43ba844764d717011d4d55497e8dbb69438e5b5d' as 'htc_helm' 374c175 6 days ago

0 contributors

92 lines (90 sloc) | 2.22 KB Raw Blame History 

```

1 kind: Service
2 apiVersion: v1
3 metadata:
4   name: tts-svc
5 spec:
```

```

42 - name: tts-cache
43   imagePullPolicy: Always
44   env:
45     - name: IAM_TOKEN
46       value: "{{ .Values.IAM_TOKEN }}"
47     - name: IAM_CLIENT_ID
48       value: "{{ .Values.IAM_CLIENT_ID }}"
49     - name: IAM_CLIENT_SECRET
50       value: "{{ .Values.IAM_CLIENT_SECRET }}"
51     - name: IAM_MAP_CLIENT_ID
52       value: "{{ .Values.IAM_SCIM_CLIENT_ID }}"
53     - name: IAM_MAP_CLIENT_SECRET
54       value: "{{ .Values.IAM_SCIM_SECRET }}"
55     - name: IAM_MAP_GROUP
56       value: "{{ .Values.IAM_MAP_GROUP }}"
57     - name: PROXY_AUDIENCE
58       value: "{{ .Values.PROXY_AUDIENCE }}"
59     - name: PROXY_TTS
60       value: "{{ .Values.PROXY_TTS }}"
61     - name: PROXY_IAM_ENDPOINT
62       value: "{{ .Values.PROXY_IAM_ENDPOINT }}"
63     - name: PROXY_CREDENTIAL_ENDPOINT
64       value: "{{ .Values.PROXY_CREDENTIAL_ENDPOINT }}"
65     - name: PROXY_LOCAL_CACHE_EXPIRATION_TIME
66       value: "86400"
67     - name: PROXY_LOCK_FILE_AGE
68       value: "20"
69     - name: PROXY_CACHE_DIR
70       value: "/tmp"
71     - name: PROXY_LOCAL_CACHE_PATH
72       value: "/tmp/tts-cache"
```

let's open HTCondor config files to see more...

```
# Security group
SEC_DEFAULT_AUTHENTICATION = REQUIRED
SEC_DEFAULT_AUTHENTICATION_METHODS = GSI
SEC_DEFAULT_INTEGRITY = REQUIRED

CERTIFICATE_MAPFILE = /etc/condor/condormapfile

GSI_DAEMON_DIRECTORY = /etc/grid-security

GSI_DAEMON_NAME = /C=IT/O=CLOUD@CNAF/CN=0931b26e-89f6-4118-a5c4-dd7f9e9ec85a@dodas-iam
GSI_DAEMON_PROXY = /root/gwms_proxy
```

```
# Condor connection broker
# Only worker node can have CCB_ADDRESS
```

```
# MASTER or SCHEDD ADDRESS
NETWORK_INTERFACE = 192.168.190.145
```

```
STARTD_DEBUG = D_ALL
# Define SLOTS
NUM_SLOTS = 1
NUM_SLOTS_TYPE_1 = 1
SLOT_TYPE_1 = cpus=1, mem=4096
[root@ccb ~]#
```

SCHEDD →

← Central Manager (+CCB)

```
# Security group
SEC_DEFAULT_AUTHENTICATION = REQUIRED
SEC_DEFAULT_AUTHENTICATION_METHODS = GSI
SEC_DEFAULT_INTEGRITY = REQUIRED

CERTIFICATE_MAPFILE = /home/uwdir/condormapfile

GSI_DAEMON_DIRECTORY = /etc/grid-security

GSI_DAEMON_NAME = /C=IT/O=CLOUD@CNAF/CN=0931b26e-89f6-4118-a5c4-dd7f9e9ec85a@dodas-iam
GSI_DAEMON_PROXY = /root/gwms_proxy
```

```
# Condor connection broker
# Only worker node can have CCB_ADDRESS
```

```
# MASTER or SCHEDD ADDRESS
NETWORK_INTERFACE = 193.204.89.85
```

```
STARTD_DEBUG = D_ALL
# Define SLOTS
```



```
condormapfile
[root@scheddpublic uwdir]# cat condormapfile
GSI "^\\C\\=IT\\O\\=CLOUD@CNAF\\CN\\=7a91e9d3-6cd0-4347-9674-ee0f15603a2d@dodas-iam$" sarac13
GSI "^\\C\\=IT\\O\\=CLOUD@CNAF\\CN\\=0931b26e-89f6-4118-a5c4-dd7f9e9ec85a@dodas-iam$" spiga
GSI "^\\C\\=IT\\O\\=CLOUD@CNAF\\CN\\=0931b26e-89f6-4118-a5c4-dd7f9e9ec85a@dodas-iam$" condor
GSI (.* ) GSS_ASSIST_GRIDMAP
GSI (.* ) anonymous
[root@scheddpublic uwdir]#
```

```
[root@scheddpublic ~]# voms-proxy-info -file gwms_proxy
subject      : /C=IT/O=CLOUD@CNAF/CN=0931b26e-89f6-4118-a5c4-dd7f9e9ec85a@dodas-iam/CN=584749314
issuer       : /C=IT/O=CLOUD@CNAF/CN=0931b26e-89f6-4118-a5c4-dd7f9e9ec85a@dodas-iam
identity     : /C=IT/O=CLOUD@CNAF/CN=0931b26e-89f6-4118-a5c4-dd7f9e9ec85a@dodas-iam
type         : RFC3820 compliant impersonation proxy
strength     : 1024
path         : /root/gwms_proxy
timeleft     : 159:47:52
key usage    : Digital Signature, Key Encipherment
[root@scheddpublic ~]#
```

(Question: but I never passed to the system my X509 certificate .. where it come from?)

do you remember the Question1: why both? isn't it two time the same thing?
do I need both?

- we need both now.. but we are moving toward Token only solution

Nowadays we have HTCondor is natively supporting Tokens... this means that we can actually avoid X509... and yes we are going beyond X509...

```
root@scheddpublic ~]# condor_version
CondorVersion: 8.9.3 Sep 25 2019 PackageID: 8.9.3-1.1 $
CondorPlatform: X86_64-CentOS_7.7 $
root@scheddpublic ~]#
```

Central Manager (+CCB)

```
#SEC_DEFAULT_INTEGRITY = REQUIRED
#SEC_DEFAULT_AUTHENTICATION = REQUIRED
SEC_DEFAULT_AUTHENTICATION_METHODS = SCITOKENS
#SEC_READ_AUTHENTICATION_METHODS = FS,SCITOKENS
#SEC_WRITE_AUTHENTICATION_METHODS = FS,SCITOKENS
#SEC_ADVERTISE_STARTD_AUTHENTICATION_METHODS = FS,SCITOKENS

SCHEDD.ALLOW_NEGOTIATOR = *
#SCHEDD.SEC_WRITE_AUTHENTICATION_METHODS = FS,SCITOKENS,GS
#SCHEDD.SEC_READ_AUTHENTICATION_METHODS = FS,SCITOKENS,GS
#COLLECTOR.SEC_READ_AUTHENTICATION_METHODS = FS,SCITOKENS,GS
#COLLECTOR.SEC_WRITE_AUTHENTICATION_METHODS = FS,SCITOKENS,GS
#COLLECTOR.SEC_ADVERTISE_STARTD_AUTHENTICATION_METHODS = FS,SCITOKENS,GS

# Condor connection broker
# Only worker node can have CCB_ADDRESS

SCITOKENS_SERVER_AUDIENCE=my-ce.example.com:9619

#STARTD_DEBUG=D_FULLDEBUG,D_SECURITY

MASTER or SCHEDD ADDRESS
```

144.1 92%

SCHEDD

```
# Host sec. policy
HOSTALLOW_ADMINISTRATOR = $(CONDOR_HOST)
HOSTALLOW_OWNER = $(FULL_HOSTNAME), $(HOSTALLOW_ADMINISTRATOR)
HOSTALLOW_WRITE_COLLECTOR = $(HOSTALLOW_WRITE), $(FLOCK_FROM)
HOSTALLOW_WRITE_STARTD = $(HOSTALLOW_WRITE), $(FLOCK_FROM)
HOSTALLOW_READ_COLLECTOR = $(HOSTALLOW_READ), $(FLOCK_FROM)
HOSTALLOW_READ_STARTD = $(HOSTALLOW_READ), $(FLOCK_FROM)

# Ports
HIGHPORT = 1084
LOWPORT = 1024
USE_SHARED_PORT = True

# Security group
#SEC_DEFAULT_INTEGRITY = REQUIRED
#SEC_DEFAULT_AUTHENTICATION = REQUIRED
SEC_DEFAULT_AUTHENTICATION_METHODS = SCITOKENS
#SEC_READ_AUTHENTICATION_METHODS = SCITOKENS
#SEC_WRITE_AUTHENTICATION_METHODS = SCITOKENS
#SEC_ADVERTISE_STARTD_AUTHENTICATION_METHODS = SCITOKENS

COLLECTOR.ALLOW_ADVERTISE_MASTER = *
COLLECTOR.ALLOW_ADVERTISE_SCHEDD = *
COLLECTOR.ALLOW_ADVERTISE_STARTD = *
```

130,1 86%

```
[root@scheddpublic condor]# cat condor_mapfile
SCITOKENS https://iam-escape.cloud.cnaf.infn.it/,241687e8-5374-4549-b9f6-a3866f0bf6da andrea@users.htcondor.org
SCITOKENS https://iam-escape.cloud.cnaf.infn.it/,e9bf50ed-16ec-4a2c-8986-9ede3d9fba45 daniele@users.htcondor.org
[root@scheddpublic condor]#
```

/UUIS.DV#11328-11348

Getting a token and that's it...

- you learned during this course how to get it (device flow... using device code)

```
spiga@spiga-XPS:~/DODAS-deployer/HTCondor-Token$ echo $ESCAPE_TOKEN
eyJraWQiOiJyc2ExIiwiaWVxanIjoIULMyNTYifQ.eyJzdWIiOiJlOWJmNTBlZC0xNmVjLTRhMmMtODk4Ni05ZWRLM2Q5ZmJhNDUiLCJhdWQiOiJteS1jZS5leGFtcGx1LmNvbTo5NjESIiwibmJmIjoxNTc0ODY1ODIxLCJzY29wZSI6ImVtYWlsIG9mZmxpbmVfYWNjZXNzIG9wZW5pZCBwcm9maWx1IiwiaXNzIjoiaHR0cHM6XC9cL2lhbS1lc2NhcnGUuY2xvdWQuY25hZi5pbmZuLm0XC8iLCJleHAiOiJlNzQ4Njk0MjEsImhhdCI6MTU3NDg2NTgyMSwianRpIjoIN2NmZBkMDgtN2Q2My00Y2MxLWl5ODEtZTU5NGY0NTQxMTgxIn0.gRIB84Xs1394QczabKG6B3Q0t7J2n-jikCtabxaRKC1gsVn0zmXk7XrL_kWLLniHjRqcRj-3hgAnjlkndztfd9u0F4QkYeLx9ostWnm03NmYOpnD2c4QKvzY55AbHBPhJPBRmimayMA20U5q1aIB3jBFUe0aRN9OCF3Viy-M5o
spiga@spiga-XPS:~/DODAS-deployer/HTCondor-Token$ echo $ESCAPE_TOKEN | cut -d '.' -f2 | base64 -d | jq -r .
base64: invalid input
{
  "sub": "e9bf50ed-16ec-4a2c-8986-9ede3d9fba45",
  "aud": "my-ce.example.com:9619",
  "nbf": 1574865821,
  "scope": "email offline_access openid profile",
  "iss": "https://iam-escape.cloud.cnaf.infn.it/",
  "exp": 1574869421,
  "iat": 1574865821,
  "jti": "7cd30d08-7d63-4cc1-b981-e594f4541181"
}
```

But where these tokens come from?

```
spiga@spiga-XPS:~/DODAS-deployer/HTCondor-Token$ echo $ESCAPE_TOKEN
eyJraWQiOiJyc2ExIiwiaWxnbG9mdG9zaXQiOiJldmVpZC9wcm9maWwlaXNzIjoiaHR0cHM6XC9cL2lhbS1lc2NhcnVzY25hZi5pbmZuLm0XC8iLCJleHAiOiE1NzQ4Njk0MjEsImh0bCI6MTU3NDg2NTgyMSwianRpIjoia2NkMzBkMDgtN2Q2My00Y2MxLWl5ODR0c2U5NGY0NTQxMTgxIn0.gRIB84Xs1394QczabKG6B3Q0t7J2n-jikCtabxaRKC1gsVn0zmXk7XrL_kWLLniHjRqcRj-3hgAnjlkndztfd9u0F4QkYeLx9ostWnm03NmYOpnD2c4QKvzY55AbHBPhJPBRmimayMA20U5q1aIB3jBFUe0aRN9OCF3Viy-M5o
spiga@spiga-XPS:~/DODAS-deployer/HTCondor-Token$ echo $ESCAPE_TOKEN | cut -d '.' -f2 | base64 -d | jq -r .
base64: invalid input
{
  "sub": "e9bf50ed-16ec-4a2c-8986-9ede3d9fba45",
  "aud": "my-ce.example.com:9619",
  "nbf": 1574865821,
  "scope": "email offline_access openid profile",
  "iss": "https://iam-escape.cloud.cnaf.infn.it/",
  "exp": 1574869421,
  "iat": 1574865821,
  "jti": "7cd30d08-7d63-4cc1-b981-e594f4541181"
}
```

li now try to impersonate Andrea Ceccanti ... so let's move [here](#)

Thank you for your attention!

Questions?



EOOSC-hub

Contact

 eosc-hub.eu  [@EOOSC_eu](https://twitter.com/EOSC_eu)



This material by Parties of the EOOSC-hub Consortium is licensed under a Creative Commons Attribution 4.0 International License.