

Manuel d'installation et d'utilisation de Google/CAPIRCA pour Telespazio (GCT)

Juan PIRON
Elève ingénieur,
4ème année *Sécurité et Technologies Informatiques*,
Insa Centre Val de Loire,
Campus de Bourges
`juan.piron@insa-cvl.fr`

3 août 2017

Table des matières

1	Prérequis	3
2	Ce qu'est Google/CAPIRCA pour TPZ	3
3	Ce que n'est pas Google/CAPIRCA pour TPZ	3
4	Présentation du logiciel	3
5	Installation	4
5.1	Prérequis	4
5.1.1	Utilisateur git	4
5.1.2	MariaDB	4
5.1.3	Python	4
5.1.4	SSH	5
5.1.5	Autres	5
5.2	Procédure	6
5.3	Déploiement	7
6	Utilisation	9
6.1	Configuration du dépôt local et du client	9
6.2	Exemple	10
6.3	Recommandations	11
7	Rappels succincts sur les commandes Git	11
8	Aller plus loin	13

1 Prérequis

Ce manuel n'a pas pour but de décrire l'architecture de Google/CAPIRCA. Ce manuel ne remplace d'aucune manière la documentation de Google/CAPIRCA, il apporte simplement les spécificités de GCT. Il est donc nécessaire de lire le README de Google/CAPIRCA. Pour cela il existe la wiki GitHub de Google/-CAPIRCA.

Toutes les adresses ips et les configurations présentes dans ce document sont fictives.

2 Ce qu'est Google/CAPIRCA pour TPZ

Capirca est un outil conçu pour utiliser des définitions communes des réseaux, des services et des fichiers de règles (politiques) de haut niveau. Cela facilite le développement et la manipulation des listes de contrôle d'accès réseau (ACL) pour diverses plates-formes. GCT est Capirca appliqué à la gestion du PGL. Il permet de rendre plus rapide la prise en charge des demandes d'ouverture de flux utilisateur.

3 Ce que n'est pas Google/CAPIRCA pour TPZ

GCT ne remplace en aucun cas le manager (Cisco ASDM). C'est à dire que toutes modifications ou suppression d'une demande ce fait avec le manager. En d'autres termes pour supprimer une ACL ajouter à l'aide de GCT :

- 1/ La supprimer dans le fichier .pol correspondant.
- 2/ Aller sur le manager et la supprimer.

Pour modifier :

- 3/ réécrire le term correspondant à l'ACL dans le .pol.
- 4/ recompiler

Ne pas utiliser GCT pour une utilisation autre que celle décrite. Si le besoin est de créer des ACLs de type iptables, juniper ou encore cisco, veuillez utiliser le Google/CAPIRCA original.

4 Présentation du logiciel

Si vous détenez ce présent document c'est que vous avez aussi l'archive GCT.tar.gz. Cette archive contient 2 dossiers. Le premier contient les fichiers sources originaux de Google/CAPIRCA plus les dossiers sync et diff. *sync/* et *diff* contiennent les différents scripts d'adaptation de Capirca au PGL de TPZ. Sync s'occupe de la synchronisation des objets et diff d'éviter les doublons. A coter de *capirca/* il y a gogsInstall qui contient tous le nécessaire pour l'installation.

5 Installation

Cette section concerne l'installation de Gogs sur le serveur (le manager) et le déploiement de GCT. L'installation décrite concerne un serveur Centos 7. Il faut avoir au moins deux interfaces réseaux. Une ayant accès à internet et l'autre étant sur le même réseau que le PGL.

5.1 Prérequis

5.1.1 Utilisateur git

Sur le serveur "manager" créer l'utilisateur git et définir son mot de passe :

```
# useradd -m git
# passwd git
```

Ajouter pour l'installation, git au groupe sudo :

```
# usermod -aG wheel git
```

Ne pas oublier de l'en retirer après l'installation. Pour tout le reste de cette installation utiliser "git".

Décompresser gogsInstall.tar.gz dans */home/git* :

```
# tar -xzf GCT.tar.gz
```

5.1.2 MariaDB

Si la bdd n'existe pas alors l'installer :

```
yum -y update
yum -y install mariadb-server
service mariadb start
mysql -u root -e "SET PASSWORD FOR 'root'@'localhost' = PASSWORD('password');"
```

5.1.3 Python

Version 2.7 ou supérieur.

Installer pip :

```
# curl "https://bootstrap.pypa.io/get-pip.py" -o "get-pip.py"
# python get-pip.py
```

Installer paramiko :

```
# yum -y install gcc libffi-devel python-devel openssl-devel
# pip install cryptography
# pip install paramiko
```

Installer netmiko :

```
# pip install scp
# pip install pyyaml
# pip install pytest
```

5.1.4 SSH

Avoir openssh-server sur le serveur et configuré ssh avec un utilisateur ssh "git" sur le PGL.

Firewall PGL :

```
hostname(config)# crypto key generate rsa modulus 1024
hostname(config)# write memory
hostname(config)# aaa authentication ssh console LOCAL
hostname(config)# username git password password
hostname(config)# ssh timeout 30
hostname(config)# ssh version 2
```

Cette exemple de configuration a été fait à partir d'une maquette qui utilise un cisco ASA 5520. Il peut donc y avoir des différences avec le PGL. Eviter d'utiliser les certificats, sinon modifier les scripts pre-receive et post-receive. Entre le client et gogs-server :

Sur un client (dans son home) :

```
# ssh-keygen -t rsa
# chmod 700 .ssh
# chmod 600 .ssh/id_rsa
# chmod 644 .ssh/id_rsa.pub
# chmod 600 .ssh/known_hosts
```

Envoyer la clé public id_rsa.pub public du poste client au server.

Sur le serveur dans un utilisateur autre que git (ex : /home/intern) :

```
# ssh-keygen -t rsa
# cat id_rsa.pub » .ssh/authorized_keys
# chmod 700 .ssh
# chmod 644 .ssh/authorized_keys
# chmod 600 .ssh/id_rsa
# chmod 644 .ssh/id_rsa.pub
```

Le serveur Gogs utilise déjà le fichier *authorized_keys* de l'utilisateur git. Il est donc nécessaire de passer par un autre utilisateur pour tous échanges ssh. Dans /etc/ssh/sshd_config désactiver PasswordAuthentication et ainsi forcer l'utilisation des clés :

```
PasswordAuthentication no
```

Ne pas oublier de relancer le serveur ssh : `systemctl sshd restart`

5.1.5 Autres

Configurer SELinux de manière à permettre l'accès à ssh (scp) au dossier tmp pour l'échange des clés.

```
# semanage permissive -a ssh_keygen_t
```

Installer Git :

```
# yum -y install git
```

Une fois Capirca importé il faut installer les prérequis dans *capirca/* à l'aide de :

```
# pip install -r requirements.txt
```

5.2 Procédure

Ce déplacer dans le dossier gogsInstall éditer les scripts python pre-receive et post-receive. L'adresse ip qui doit être rentrer et celle du PGL, de même que le couple id/password ssh :

```
pgl = {
    'device_type':'cisco_asa',
    'ip':'192.168.1.1',
    'username':'intern',
    'password':'tpzinsacv1',
    'secret':'tpzinsacv1',
}
```

Editer app.ini, faire correspondre l'adresse ip et le domain avec ceux du serveur :

```
[server]
PROTOCOL = http
DOMAIN = 192.168.1.10
ROOT_URL = %(PROTOCOL)s://%(DOMAIN)s:%(HTTP_PORT)s/
HTTP_ADDR = 192.168.1.10
```

Dans *capirca/* éditer run.sh et sync.sh, modifier en début de script les variable ip et user qui doivent contenir l'adresse ip du serveur Gogs et le nom de l'utilisateur contenant les clés ssh. Ajouter les droits d'execution au script gogsInstall.sh :

```
# chmod u+x gogsInstall.sh
```

Exécuter le script en spécifiant le mot de passe root de mariadb comme arg1. Spécifier le mot de passe que vous voulez donner à l'utilisateur git de mariadb en arg2 :

```
# ./gogsInstall.sh mdp-root-mariadb mdp-git-mariadb
```

Ouvrir un navigateur et rentrer l'url : `http://ip-du-serveur:3000`

Une page d'installation s'ouvre, il suffit d'entrer le mot de passe de l'utilisateur git de la bdd mariadb et de confirmer.

Install Steps For First-time Run

If you're running Gogs inside Docker, please read [Guidelines](#) carefully before you change anything in this page!

Database Settings

Gogs requires MySQL, PostgreSQL, SQLite3, MSSQL or TiDB.

Database Type *

MySQL

Host *

127.0.0.1:3306

User *

git

Password *

Database Name *

gogs

Please use INNODB engine with utf8_general_ci charset for MySQL.

5.3 Déploiement

Sign In

Welcome! We're glad that you chose Gogs, have fun and take care.

Username or email *

Password *

☐ Remember Me

Sign In

[Forgot password?](#)

[Need an account? Sign up now.](#)

Pour l'utilisation de Gogs se référer à sa documentation. Créer un utilisateur "tpz". A l'aide de tpz ajouter un repository distant nommer "GCT".

.gitignore

Select .gitignore templates

License

Select a license file

Readme ?

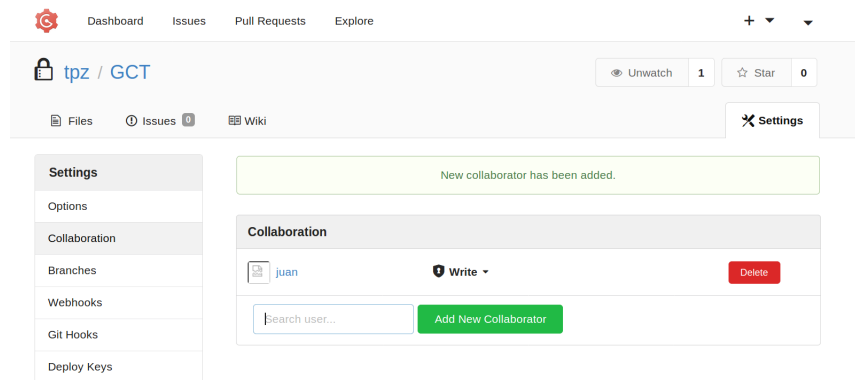
Default

☒ Initialize this repository with selected files and template

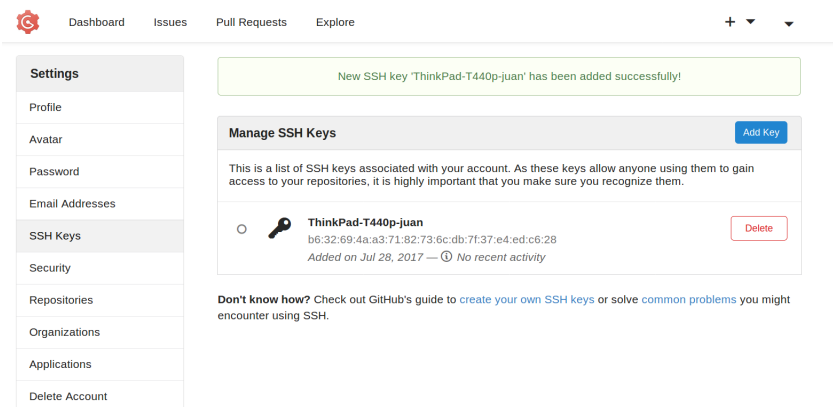
Create Repository

Cancel

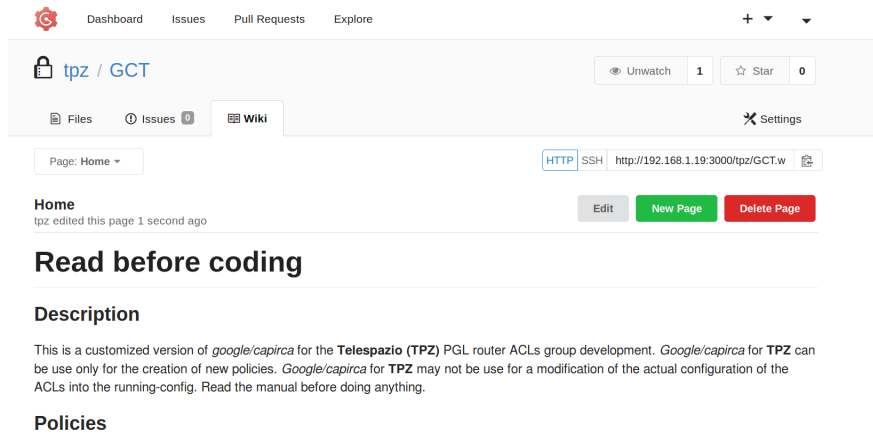
Créer d'autres utilisateurs et les incorporer comme participant en "rw".



Récupérer les différentes clés ssh des postes qui cloneront GCT et les ajouter à tpz en allant dans ses paramètres. Ne pas les ajouter au repository mais bien directement dans les paramètres de l'utilisateur tpz.



Ajouter les deux scripts python, **pre-receive** et **post-receive**, dans `/home/git/gogs-repositories/tpz/gct.git/hooks/`. Enfin récupérer la wiki dans `gogsInstall/` et l'ajouter au repository GCT.



6 Utilisation

6.1 Configuration du dépôt local et du client

Avant tout transférer sa clé rsa (ssh) à l'admin. L'étape suivante et de configurer localement Git à l'aide de :

```
# git config -global user.name "John Doe"
# git config -global user.email johndoe@example.com
```

Le nom spécifié sera celui qui apparaîtra sur les commits. Faire ensuite un clone du dépôt distant en local :

```
# git clone ssh://git@192.168.1.10:2222/tpz/GCT.wiki.git
```

Si c'est le premier client créé : récupérer le dossier capirca et l'ajouter au repertoire git *GCT*/ du client, puis :

```
# git add -A
# git commit -a -m "first commit"
# git push origin master
```

Pour une demande d'ouverture de flux utilisateur créer autant de fichier .pol qu'il y a d'interfaces du PGL concernées. Dans le header le champ **target::** doit avoir pour nom celui de l'interface. Capirca ne comprend que les objets, que cela soit pour les réseaux ou les services. Avant de créer un .pol il faut donc créer les objets. Pour les réseaux les ajouter en début du fichier *capirca/def/NETWORK.net* et pour les services dans *capirca/def/SERVICES.svc*. GCT récupère de manière automatique les objets présent sur le PGL, donc regarder d'abord si l'objet existe en faisant un CTRL-F en spécifiant l'ip ou le service. Les demandes au format .pol doivent se trouver dans le dossier *capirca/policies/pol*. Après avoir terminer de créer les différents fichier .pol, dans *capirca/* lancer le script : `./run.sh`

Quand on vous le demandera, entrer un commit. Tous les commits doivent être de la forme : `ajout de ref-de-la-demande` ou `modification de ref-de-la-demande`.

Pour une suppression ou modification faire comme indiqué dans *Ce que n'est pas GCT*.

Récapitulation :

- 1/ Rechercher ou créer les objets
- 2/ Créer les .pol
- 3/ ./run.sh

Si lors de la compilation (abus de langage) il se produit un Git "CONFLICT" se référer à la partie *Rappels succints sur les commandes Git*. Avant tout essai assurez-vous d'avoir bien toutes les librairies python requises d'installées et Git :

- gflags (pip install python-gflags)
- netaddr (pip install netaddr)
- Git (yum -y install git)

6.2 Exemple

Voici un exemple de configuration d'une demande .pol et des objets.

```
----- .POL -----

header {
    comment:: "Demandeur : Tintin"
    comment:: "Realisee par : Cpt. Hadock"

    target:: ciscoasa Eth1_CSG
}

term NTP {
    source-address:: REMUS1
    protocol:: udp
    source-port:: NTP_SOURCE
    destination-address:: REMUS2
    destination-port:: NTP_DEST
    logging:: syslog
    action:: accept
}

term SYSLOG {
    source-address:: A_192_168_1_2
    protocol:: udp
    source-port:: SYSLOG_SOURCE
    destination-address:: SSI
    destination-port:: SYSLOG_DEST
}
```

```

        logging:: syslog
        action:: accept
    }

----- NETWORK.net -----

REMUS1 = 192.168.10.0/24
REMUS2 = 192.168.20.0/24
REMUS10 = 192.168.100.0/24
REMUS11 = 192.168.110.0/24
A_192_168_1_2 = 192.168.1.2/32
SSI = 192.168.30.0/24

----- SERVICES.svc -----

NTP_SOURCE = 123/udp
NTP_DEST = 123/udp
SYSLOG_SOURCE = 514/udp
SYSLOG_DEST = 1024-65535/udp
Netbios-src = 135/tcp
              139/tcp
Netbios-dest = 1024-65535/tcp

```

6.3 Recommandations

Ne pas utiliser de caractères spéciaux. Ne pas utiliser de : slash, backslash ou d'accents. Ne pas écrire de `remark::` trop longue, la limite est de 50 caractères.

7 Rappels succincts sur les commandes Git

En cas de conflit Git c'est toujours mieux de se souvenir des commandes importantes.

```

git init : initialise un repertoire vide
git clone https://... : récupère un projet (correspond à un fetch + un merge)

```

En local :

```

git add fichier.txt
git add -A : tous
git commit fichier.txt -m blablabla ou git commit -a blabla
git commit -amend : modifier le dernier commit (ex : faute de frappe).

```

Travail avec un dépôt distant :

`git remote add origin https://...` : ajout d'un dépôt distant, origin correspond au nom que l'on donne au dépôt
`git remote -v` : liste les repos distants (dépôts)
`git remote rm origin` : supprime le remote origin
`git pull origin master` : mise à jour avec la branche master du dépôt origin
`git push origin master` : on envoie à la branche master du dépôt origin nos modifs

Les branches :

`git branch test` : créer une branche test en local
`git branch` : liste les branches présentes
`git push origin test` : permet de pusher sur la nouvelle branche mais aussi de la créer sur le dépôt distant
`git checkout test` : permet de switcher entre les différentes branches
`git merge test` : depuis la branche master, permet de fusionner le travail de la branche test
`git push origin -delete test` : supprime la branche dans le rep distant
`git branch -d test` : supprime la branche localement

Le stash :

`git stash` : pour mettre de côté un travail que l'on ne veut pas commit si on doit changer de branch
`git stash apply` ou `git stash apply stash@{0}` : pour le récupérer au retour
`git stash list` : affiche la pile
`git stash drop stash@{0}` : supprime le stash
`git stash pop` : pour appliquer la remise puis la supprimer

Les différences :

`diff master origin/master` : différence entre la branche local et celle dans le rep distant

Revenir en arriere :

`git log` : lister les commits (et voir le num)
`git checkout <commit>` : revenir au commit indiqué comme spectateur
`git reset -hard` : revenir au dernier commit
`git reset <commit> -hard` : revenir au commit indiqué

Les différentes copies dans gits :

workspace, index, local repository, remote repository

add : workspace -> index

commit : index -> local

push : local -> remote

fetch : remote -> local

merge : local -> workspace

pull : remote -> workspace

8 Aller plus loin

Cette version de GCT doit être considérée comme une version beta. C'est à dire une première version. Il y'a plusieurs améliorations possibles. Permettre la modification et la suppression, directement depuis GCT, des ACLs créées à l'aide de GCT. Compléter les différents cas possible d'ACLs dans regexObjects.py. Et pourquoi pas, ajouter une interface plus ergonomique.