



SSHGATE

PATRICK GUIRAN

pguiran@linagora.com

SOMMAIRE

I. PROBLÉMATIQUE DES ACCÈS

II. PRÉSENTATION DE SSHGATE

III. FONCTIONNEMENT INTERNE

SOMMAIRE

I. PROBLÉMATIQUE DES ACCÈS

II. PRÉSENTATION DE SSHGATE

III. FONCTIONNEMENT INTERNE

I. PROBLÉMATIQUE DES ACCÈS

DIFFÉRENTS TYPES D'ACCÈS

- Accès par mot de passe
 - Utilisation d'un annuaire LDAP
 - Effet « post-it »
 - Partagé entre administrateurs
 - ...ou possédé par un seul administrateur (spof)

- Accès par clé ssh
 - A qui est la clé?
 - Ajout des clés du « copain » (solvable)

- Accès à l'ensemble des serveurs
 - Même les plus critiques (mail, base de données)
 - ...Souvent de manière inconditionnelle

I. PROBLÉMATIQUE DES ACCÈS

GESTION DES ACCÈS

- Arrivé / Départ d'un collaborateur ?
- Qui a accès au serveur ? (simple)
- A quel serveur a accès cet administrateurs ? (compliqué)
 - « Simple » lorsque l'administrateur a accès à tous les serveurs 😊
 - Bon administrateur : « Mais si c'est simple ! »

```
user_sshkey=$( cat user-sshkey.pub )
for serveur in $( cat list-server.txt ) ; do
  ssh $serveur 'cat ~/.ssh/authorized_keys2?' \
    | grep ${user_sshkey} >/dev/null
  [ $? -eq 0 ] && echo "${serveur}"
done
```

- Qui gère les accès?

I. PROBLÉMATIQUE DES ACCÈS

BESOINS DE LINAGORA

- Must have
 - ✓ Utilisation de ssh
 - ✓ Authentification par clé ssh
 - ✓ Que les clés des utilisateurs ne soient pas sur les serveurs
 - ✓ Gestion des accès centralisée (ACL)

- Nice to have
 - ✓ Enregistrement de l'activité des utilisateurs
 - ✓ Enregistrement des sessions des utilisateurs
 - ✓ Notification des actions d'administration

I. PROBLÉMATIQUE DES ACCÈS

RECHERCHE D'UNE SOLUTION



Wallix AdminBastion

- Solution française, propriétaire, ssh/telnet/rdp



Observe-it

- Solution américaine, propriétaire, ssh/telnet/rdp



sshProxy

- Projet Open-Source (GPLv2), python, client lourd
- inactif depuis 2008(?), impossible à télécharger sur le site officiel



AdminProxy

- Projet Open-Source, commandé par l'État Français
- Projet sur 2 ans. Fin prévu en 09/2010
- Où sont les sources ? ☹

I. PROBLÉMATIQUE DES ACCÈS

RÉSULTAT DES RECHERCHES

- Aucune solution ne convient

- Trop chère
- Trop intrusif
- Non disponible

- ⇒ Développement de sshGate !

- En version libre et open-source
- Utilisable rapidement
- Simple

I. PROBLÉMATIQUE DES ACCÈS

CONTRAINTES & DÉFIS

- Se reposer sur les outils existants : OpenSSH, putty
 - Aucune installation sur les serveurs administrés
 - Aucune installation nécessaire sur les postes clients

- Multiplate-forme
 - Le serveur sshGate
 - Les serveurs administrés
 - Les postes clients

- Pas de patches sur le serveur sshGate (patch sshd)

- Léger, peu de dépendances logicielles (pas de BDD)

SOMMAIRE

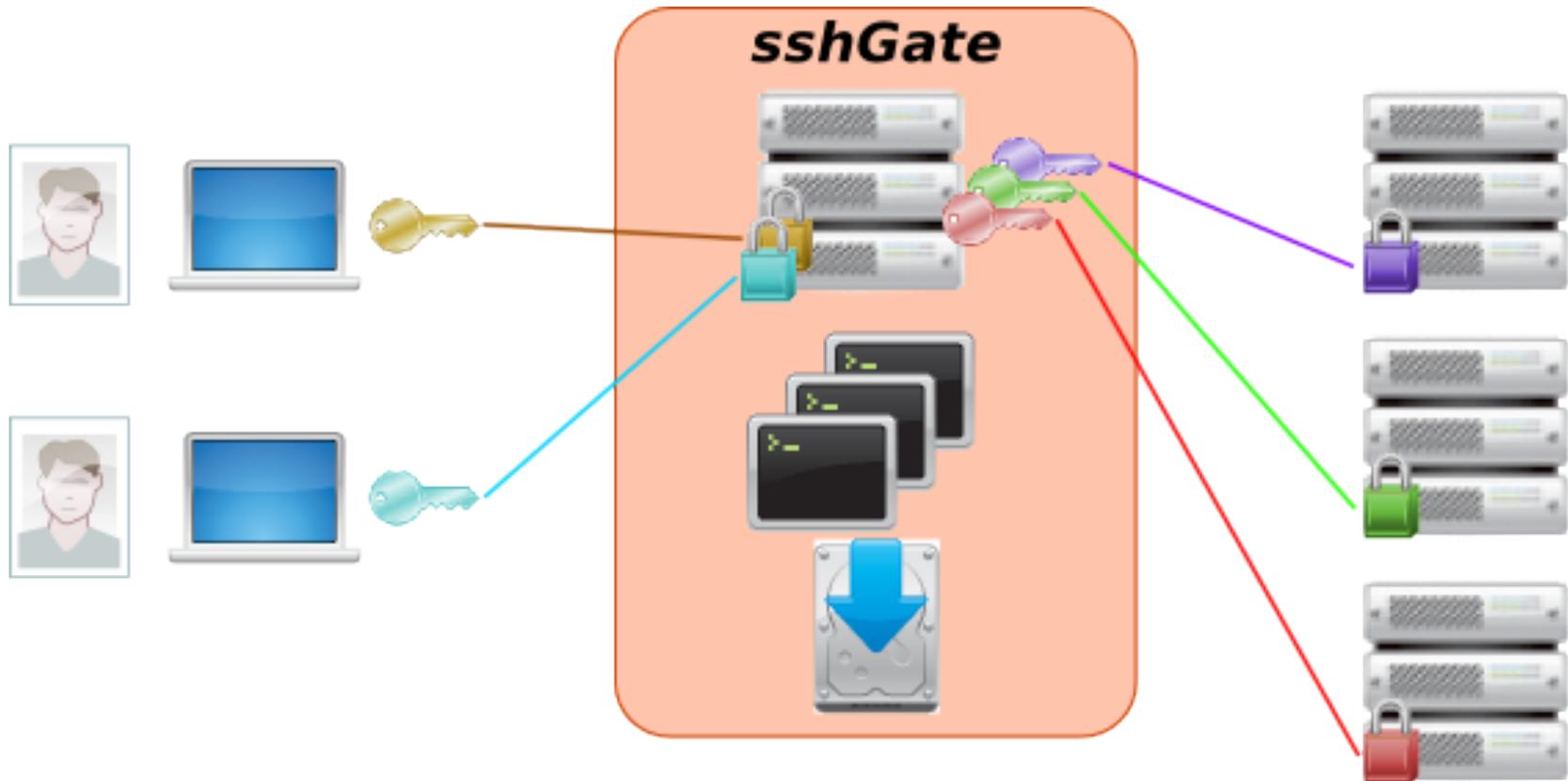
I. PROBLÉMATIQUE DES ACCÈS

II. PRÉSENTATION DE SSHGATE

III. FONCTIONNEMENT INTERNE

II. PRÉSENTATION DE SSHGATE

VUE GLOBALE



II. PRÉSENTATION DE SSHGATE

FONCTIONNALITÉS

- ✓ Sessions SSH & Transfert de fichiers via SCP
- ✓ Gestion centralisée des accès (par utilisateur et groupe)
- ✓ Gestion des alias pour les serveurs administrés
- ✓ Support multi-login par serveur administré
- ✓ Configuration SSH globale, et spécifique par serveurs et login
- ✓ Enregistrement de l'activité des utilisateurs
 - Qui fait « quoi » sur quelle machine ?
- ✓ Enregistrement des sessions SSH
 - Que s'est-il passé durant une session ?
- ✓ Interface d'administration en mode « CLI »

II. PRÉSENTATION DE SSHGATE

CARACTÉRISTIQUES

- Licence GPLv2+
- Développé en Shell Script (sh, dash, bash, zsh)

- Multiplate-forme :
 - Serveur : Linux, Solaris, *BSD
 - Client : Linux, MacOS, Windows/Putty

- Historique :
 - Naissance du projet : Août 2010
 - Première mise en production : Septembre 2010

- Version actuelle (interne) :
 - En production : 0.1.192
 - Trunk : 0.2.71 (passage en production imminente)
 - Release 1.0 prévu pour fin juillet 2011

II. PRÉSENTATION DE SSHGATE

UTILISATION DE SSHGATE PAR LINAGORA

- Quelques chiffres
 - 61 utilisateurs
 - 10 groupes d'utilisateurs
 - 161 machines administrées
 - 214 nom d'alias de machines administrées

- Accès
 - 96 accès par groupe
 - 103 accès par utilisateur

- Sur les 6 derniers mois
 - 2063 transferts de fichiers
 - 16568 sessions SSH

II. PRÉSENTATION DE SSHGATE

BUGS CONNUS & FONCTIONNALITÉS DEMANDÉES

- DOS : remplissage des logs
 - Surveillance de l'évolution de la taille des logs
 - Déconnexion des sessions abusives
- Saturation du nombre de fd ouvert
 - Limiter le nombre de connexion par utilisateur
 - Killer les sessions « idle » trop longue
- Possibilités de « cacher » certaines commandes

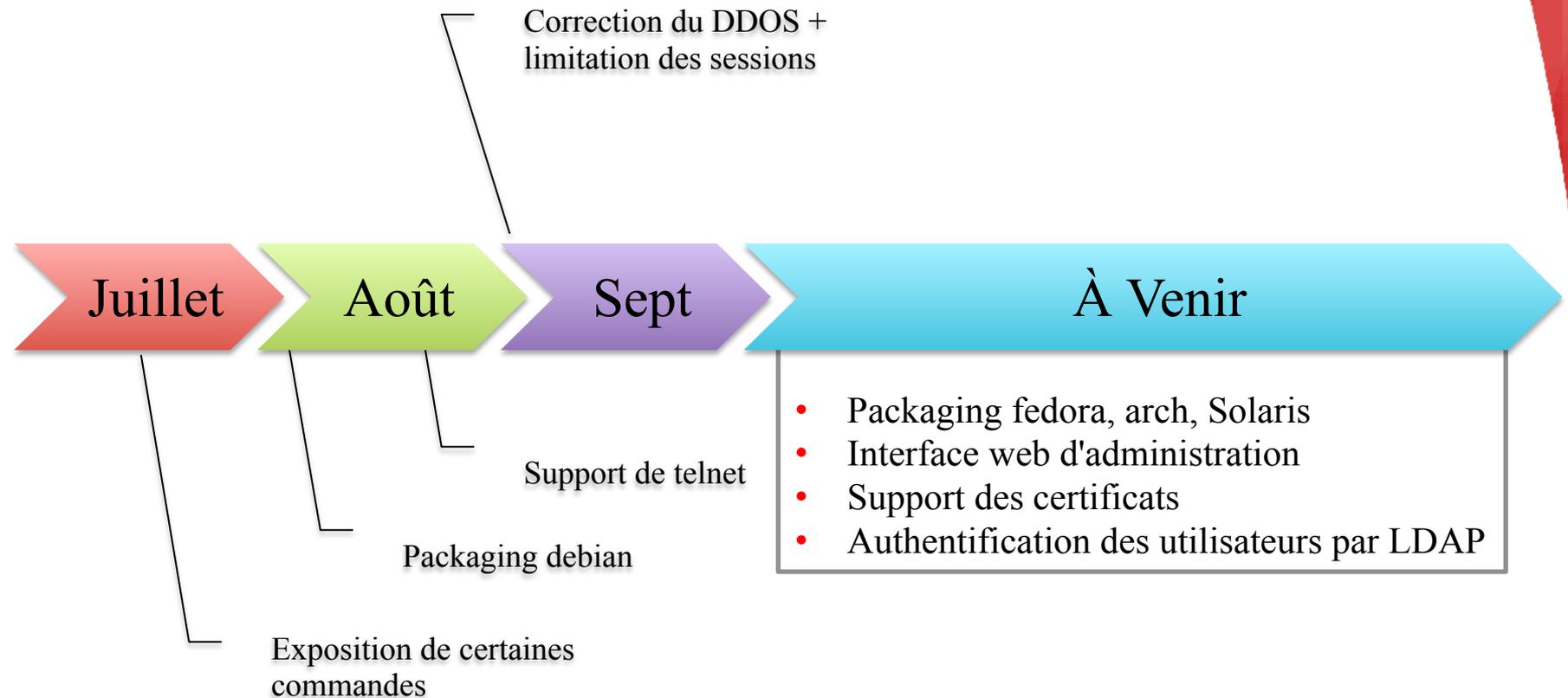
```
user@host $ read -s var          # rm -rf *  
user@host $ eval "${var}"       # AIE
```

Ce n'est pas un bug.

sshGate n'enregistre pas les touches tapées et ne le fera jamais !

II. PRÉSENTATION DE SSHGATE

ROADMAP



SOMMAIRE

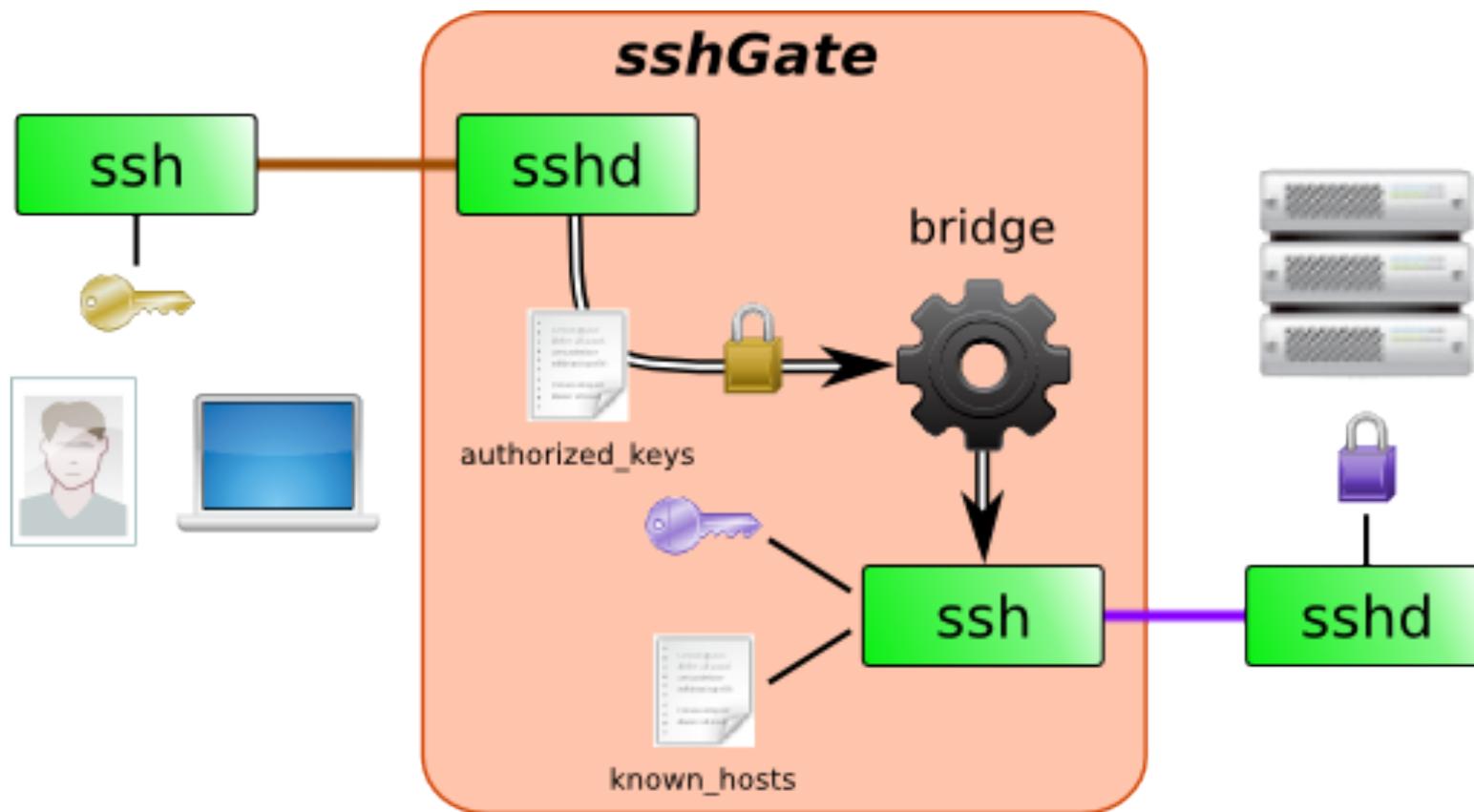
I. PROBLÉMATIQUE DES ACCÈS

II. PRÉSENTATION DE SSHGATE

III. FONCTIONNEMENT INTERNE

III. FONCTIONNEMENT INTERNE

FONCTIONNEMENT D'UNE SESSION



III. FONCTIONNEMENT INTERNE

DÉROULEMENT D'UNE OUVERTURE DE SESSION

- Connexion de l'utilisateur
 - Vérification de la présence de sa clé
 - Exécution du Bridge et passage du login + SSH_ORIGINAL_COMMAND

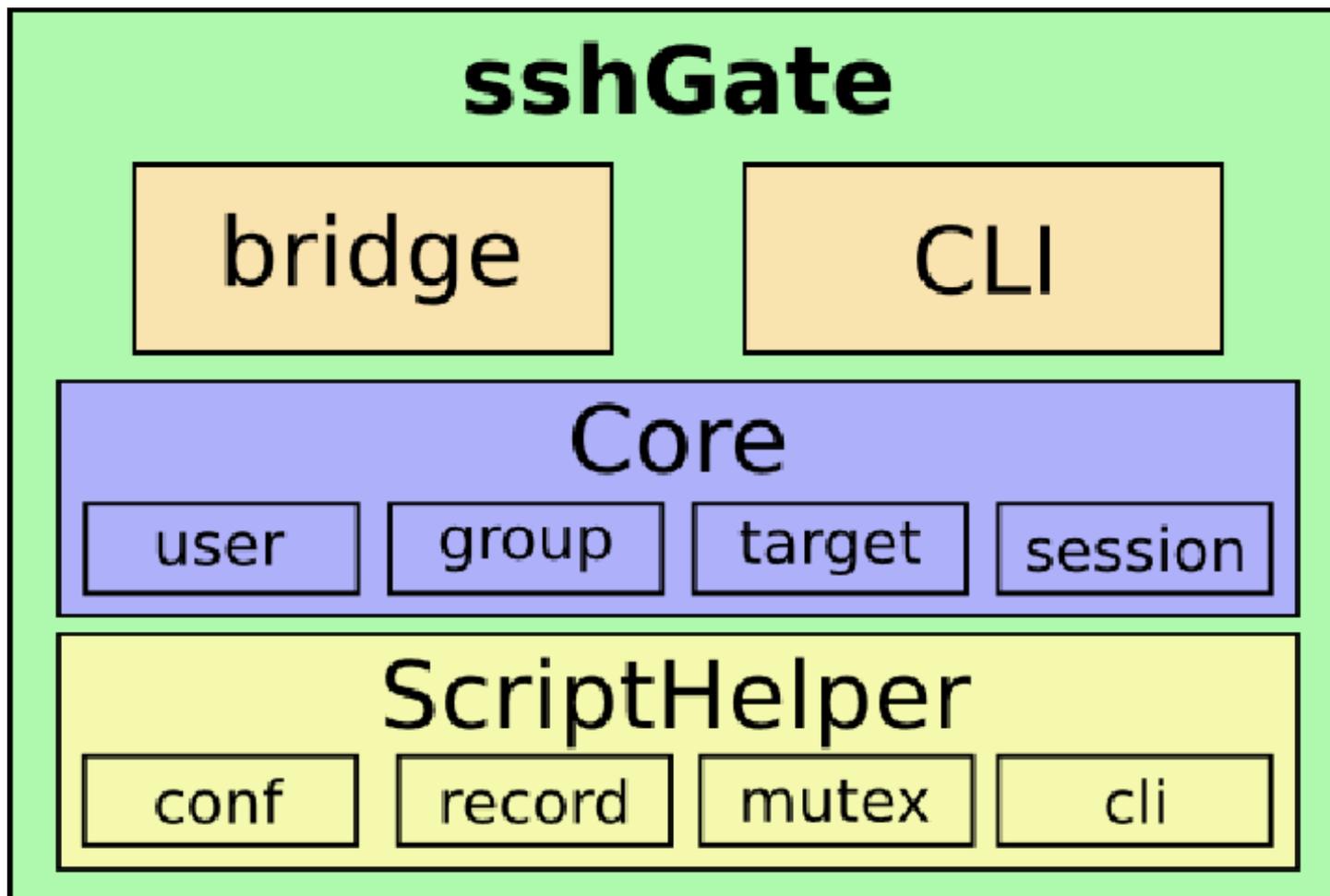
- Vérification de l'existant de l'utilisateur dans sshGate

- Parsing du SSH_ORIGINAL_COMMAND
 - Extraction du nom de la machine administrée cible
 - Extraction de la commande à effectuer (si présence)
 - Si aucun nom de machine cible n'est fournis, passage en mode interactif

- Si machine administrée cible existe
 - Lancement de l'action demandé (ssh ou scp)
 - Avec vérification de l'authenticité de la machine cible (known_hosts)

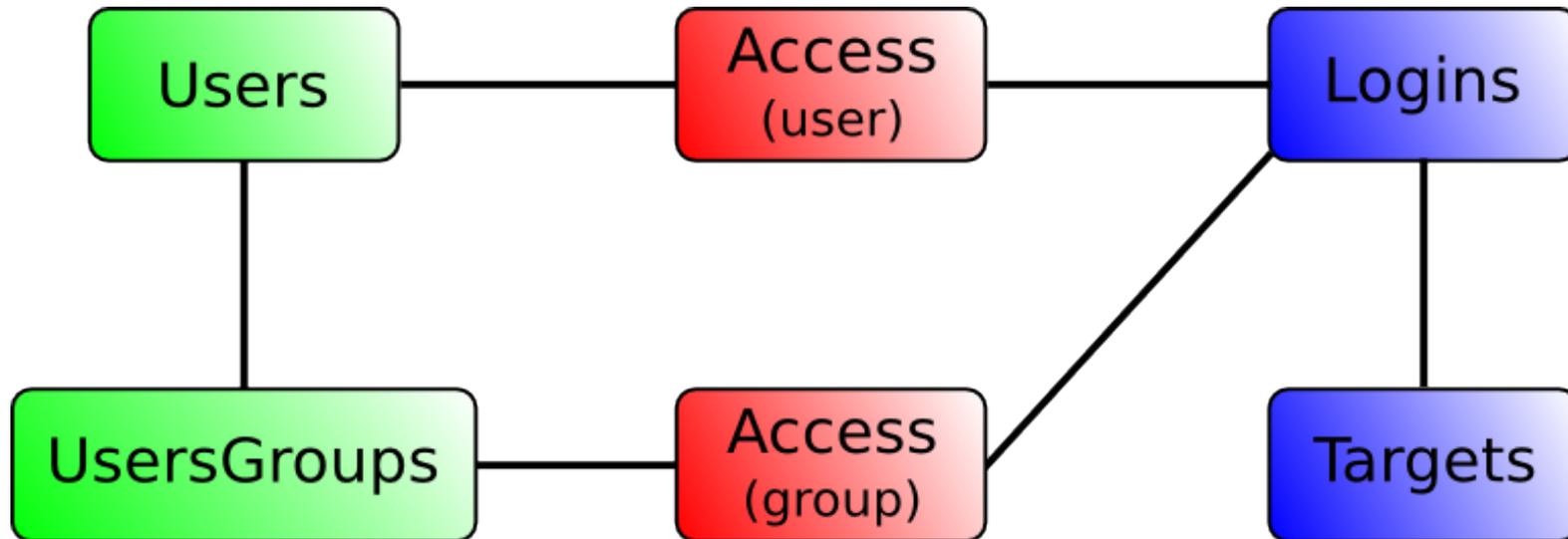
III. FONCTIONNEMENT INTERNE

ARCHITECTURE LOGICIELLE



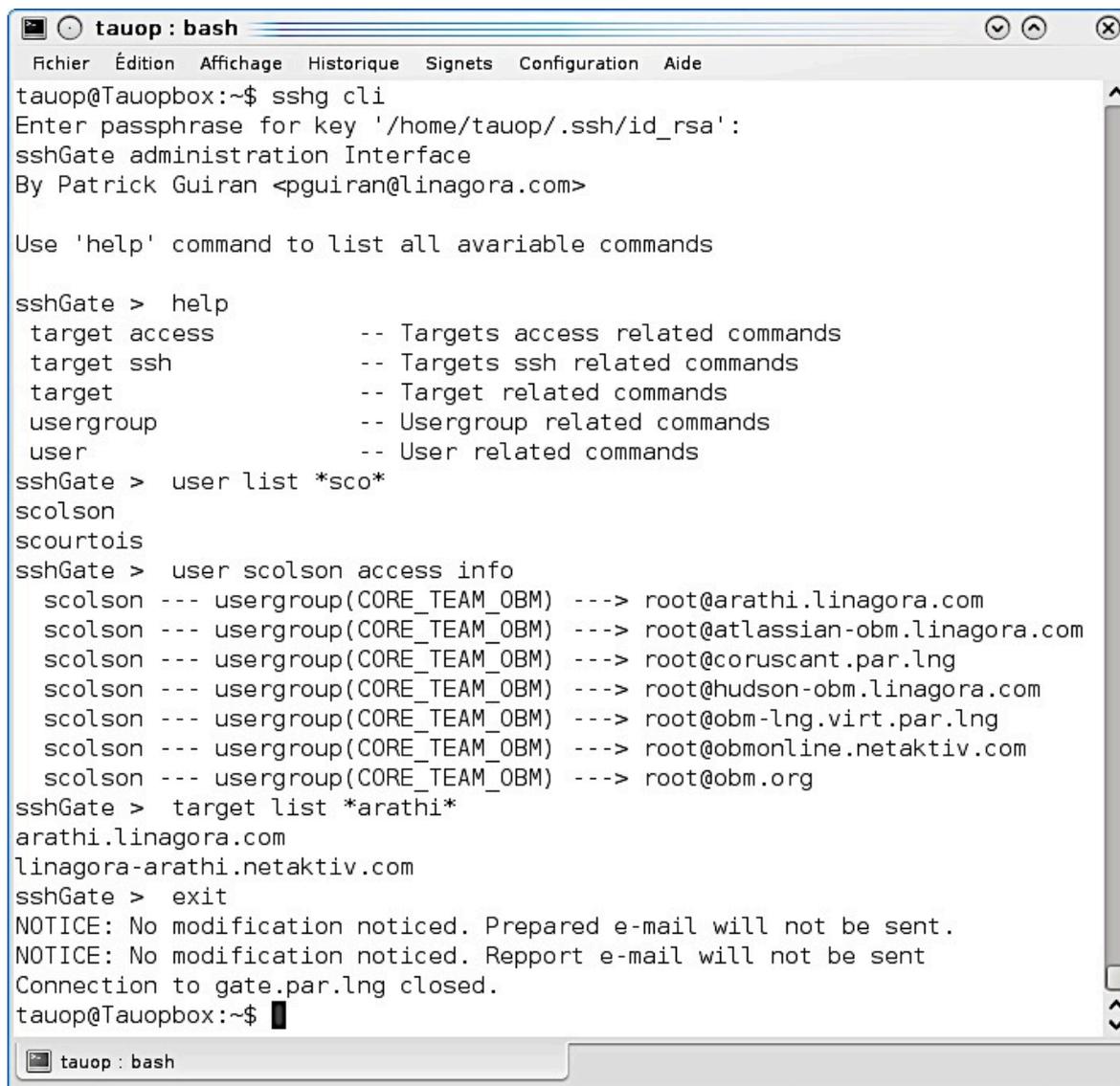
III. FONCTIONNEMENT INTERNE

ADMINISTRATION - MODÈLE DE DONNÉES



III. FONCTIONNEMENT INTERNE

CLI D'ADMINISTRATION



```
tauop : bash
Fichier  Édition  Affichage  Historique  Signets  Configuration  Aide
tauop@Tauopbox:~$ sshg cli
Enter passphrase for key '/home/tauop/.ssh/id_rsa':
sshGate administration Interface
By Patrick Guiran <pguiran@linagora.com>

Use 'help' command to list all available commands

sshGate > help
target access      -- Targets access related commands
target ssh        -- Targets ssh related commands
target            -- Target related commands
usergroup         -- Usergroup related commands
user              -- User related commands
sshGate > user list *sco*
scolson
scourtois
sshGate > user scolson access info
scolson --- usergroup(CORE_TEAM_OBM) ---> root@arathi.linagora.com
scolson --- usergroup(CORE_TEAM_OBM) ---> root@atlassian-obm.linagora.com
scolson --- usergroup(CORE_TEAM_OBM) ---> root@coruscant.par.lng
scolson --- usergroup(CORE_TEAM_OBM) ---> root@hudson-obm.linagora.com
scolson --- usergroup(CORE_TEAM_OBM) ---> root@obm-lng.virt.par.lng
scolson --- usergroup(CORE_TEAM_OBM) ---> root@obmonline.netaktiv.com
scolson --- usergroup(CORE_TEAM_OBM) ---> root@obm.org
sshGate > target list *arathi*
arathi.linagora.com
linagora-arathi.netaktiv.com
sshGate > exit
NOTICE: No modification noticed. Prepared e-mail will not be sent.
NOTICE: No modification noticed. Report e-mail will not be sent
Connection to gate.par.lng closed.
tauop@Tauopbox:~$
```

III. FONCTIONNEMENT INTERNE

BIBLIOTHÈQUE SCRIPTHELPER

- Ensemble de bibliothèques
 - Permettant d'écrire plus rapidement les Scripts Shell
 - Se voulant le plus POSIX possible

- Quelques bibliothèques
 - `exec.lib.sh` : exécution avec log et vérification
 - `ask.lib.sh` : poser des questions
 - `cli.lib.sh` : permet de construire une CLI rapidement
 - `mutex.lib.sh` / `lock.lib.sh` : gestion des verrous
 - `record.lib.sh` : enregistrement de terminal
 - ...

III. FONCTIONNEMENT INTERNE

UTILISATION DE ASK.LIB.SH

```
ASK SSHGATE_TARGETS_DEFAULT_SSH_LOGIN \  
    "what the default user account to use when connecting to target host ?" \  
    "${SSHGATE_TARGETS_DEFAULT_SSH_LOGIN}"  
  
CONF_SAVE SSHGATE_TARGETS_DEFAULT_SSH_LOGIN  
  
ASK --yesno SSHGATE_MAIL_SEND \  
    "Activate mail notification system [Yes] ?" \  
    "Y"  
[ "${SSHGATE_MAIL_SEND}" = 'N' ] && SSHGATE_MAIL_SEND='false'  
if [ "${SSHGATE_MAIL_SEND}" = 'Y' ]; then  
    SSHGATE_MAIL_SEND='true'  
    ASK SSHGATE_MAIL_TO \  
        "who will receive mail notification (comma separated mails) ?" \  
        "${SSHGATE_MAIL_TO}"  
    [ -z "${SSHGATE_MAIL_TO}" ] && SSHGATE_MAIL_SEND='false'  
else  
    SSHGATE_MAIL_SEND='false'  
fi  
CONF_SAVE SSHGATE_MAIL_SEND  
CONF_SAVE SSHGATE_MAIL_TO
```

III. FONCTIONNEMENT INTERNE

UTILISATION DE CLI.LIB.SH

```
# chargement de ScriptHelper
. ./lib/cli.lib.sh

# génération de l'aide et de son menu
CLI_REGISTER_HELP    '/tmp/sshgate-cli-help.txt' \
                      SSHGATE_GET_HELP          \
                      SSHGATE_DISPLAY_HELP       \
                      SSHGATE_DISPLAY_HELP_FOR

CLI_REGISTER_MENU    'user'                    'User related commands'
CLI_REGISTER_COMMAND 'user list'                'USERS_LIST'
CLI_REGISTER_COMMAND 'user list <pattern>'      'USERS_LIST \1'
CLI_REGISTER_COMMAND 'user add <user> mail <email>' 'USER_ADD \1 \2'
CLI_REGISTER_COMMAND 'user del <user>'          'USER_DEL \1'
CLI_REGISTER_COMMAND 'user build auth_keys'     'USERS_AUTH_KEYS_BUILD'

# ....

# lancement de la CLI
CLI_RUN
```

III. FONCTIONNEMENT INTERNE

INDUSTRIALISATION

- SshGate et ScriptHelper possèdent
 - Construction d'une tarball de déploiement
 - Script de déploiement / installation
 - Des jeux de tests

```
tauop@Tauopbox:~/taff/.../sshGate$ ./build.sh server
sshgate version ? 0.2
sshGate build number ? 014
Include ScriptHelper in package ? y
- Build sshgate-server package ... OK
tauop@Tauopbox:~/taff/.../sshGate$
```

III. FONCTIONNEMENT INTERNE

INSTALLATION (1 / 2)

```
tauop@Tauopbox:/tmp/sshGate-server-0.2-0.71$ sudo ./install.sh
```

```
--- sshGate server installation ---  
by Patrick Guiran
```

```
NOTICE: ScriptHelper will be installed as part of sshGate, not system-wide  
If you want to install ScriptHelper system-wide, please visit http://github.com/Tauop/ScriptHelper
```

```
Where do you want to locate sshGate [/opt/sshgate] ?  
Which unix account to use for sshGate users [sshgate] ?  
What the default user account to use when connecting to target host [root] ?  
List of avariable languages: fr us  
Default language for user messages [us] ? fr  
Which editor to use [vim] ?  
Activate mail notification system [Y] ?  
Who will receive mail notification (comma separated mails) [sshgate@linagora.com] ?  
Do users have to accept TOS when connecting for the first time [Y] ?  
Allow remote command [Y] ?  
Allow remote administration CLI [Y] ?
```

```
- Reload configuration ... OK  
- Installing sshGate ... OK  
- Generate default sshkey pair ... OK  
- Setup files permissions ... OK  
- Install archive cron ... OK
```

III. FONCTIONNEMENT INTERNE

INSTALLATION (2 / 2)

```
tauop@Tauopbox:/tmp/sshGate-server-0.2-0.71$ sudo ./install.sh
```

```
...
```

You need to add the first user of sshGate, which will be sshGate administrator.

This user will allow you to manage other users, targets and accesses.

```
user login ? pguiran
```

```
user mail ? pguiran@linagora.com
```

In order to administrate sshGate, just ssh this host with this user

If you have installed sshGate client -> sshg cli

with standard ssh client -> ssh -t sshgate@Tauopbox cli

from this terminal -> /opt/sshgate/bin/sshgate-cli -u sshgate

NOTICE: You may add /opt/sshgate/bin in your PATH variable

```
tauop@Tauopbox:/tmp/exmapple/sshGate-server-0.2-0.71$
```

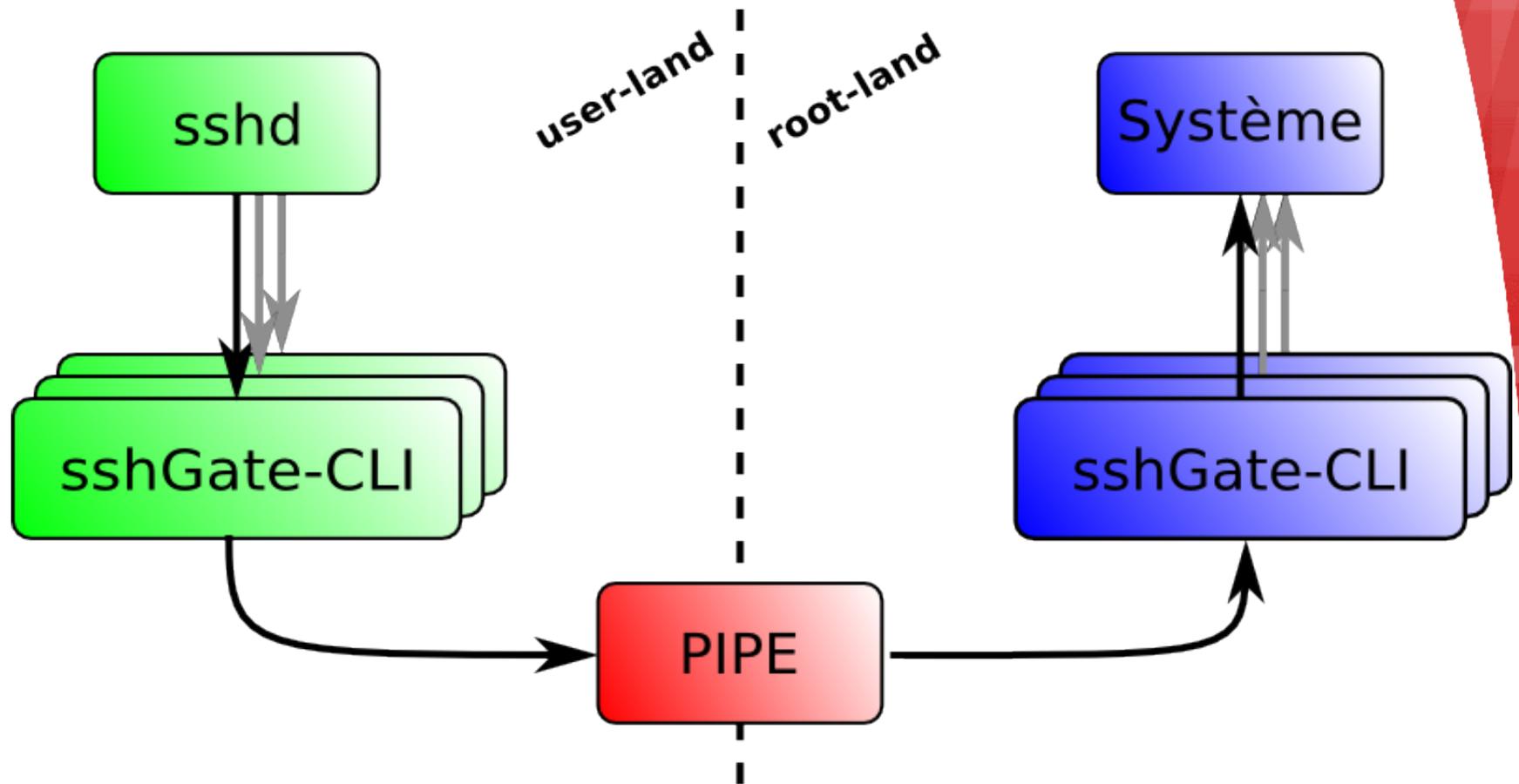
III. FONCTIONNEMENT INTERNE

TESTS

```
root@gate:/opt/sshgate/bin/tests# ./test.sh all
- Loading sshGate core ... OK
- Setup sshGate data directory ... OK
- Generate temporary test file ... OK
- Generate temporary sshkey test file ... OK
- Create and setup temporary Unix account ... OK
- Reset temporary test file ... OK
- Reset sshGate data directories ... OK
- Generate user tests ... OK
- Launch user tests ... OK
- Reset temporary test file ... OK
- Reset sshGate data directories ... OK
- Generate target tests ... OK
- Launch target tests ... OK
- Reset temporary test file ... OK
- Reset sshGate data directories ... OK
- Generate usergroup tests ... OK
- Launch usergroup tests ... OK
- Reset temporary test file ... OK
- Reset sshGate data directories ... OK
- Generate access tests ... OK
- Launch access tests ... OK
- Remove tests data ... OK
root@gate:/opt/sshgate/bin/tests#
```

IV. RÉUTILISATION DE SSHGATE

RECYCLAGE DU PROJET SSHGATE



IV. RÉUTILISATION DE SSHGATE

PARTICIPER 😊



Tauop

[Dashboard](#)

[Inbox](#) 0

[Account Settings](#)

[Log Out](#)

[Explore GitHub](#)

[Gist](#)

[Blog](#)

[Help](#)



😊 [Tauop](#) / [sshGate](#)

[Admin](#)

[Unwatch](#)

[Pull Request](#)

[3](#)

[3](#)

Source

[Commits](#)

[Network](#)

[Pull Requests \(0\)](#)

[Fork Queue](#)

[Issues \(6\)](#)

[Wiki \(7\)](#)

[Graphs](#)

Branch: `master`

[Switch Branches \(1\)](#)

[Switch Tags \(0\)](#)

[Branch List](#)

Tools to configure and use a ssh proxy server — [Read more](#)

[click here to add a homepage](#)

[Downloads](#)

SSH

HTTP

Git Read-Only

`git@github.com: Tauop/sshGate.git`



This URL has **Read+Write** access

update README for sshg



Tauop (author)

April 19, 2011

```
commit 5b074cd4b24b47db005b
tree 2769c7bbd7454b2b9fd6
parent cbe9a615d6728ba3bc0f
```

[sshGate](#) /

name

age

message

[history](#)

IV. RÉUTILISATION DE SSHGATE

PARTICIPER 😊



Tauop

[Dashboard](#)

[Inbox](#) 0

[Account Settings](#)

[Log Out](#)

[Explore GitHub](#)

[Gist](#)

[Blog](#)

[Help](#)



😊 [Tauop](#) / [ScriptHelper](#)

[Admin](#)

[Unwatch](#)

[Pull Request](#)

[3](#)

[2](#)

Source

[Commits](#)

[Network](#)

[Pull Requests \(0\)](#)

[Fork Queue](#)

[Issues \(2\)](#)

[Wiki \(0\)](#)

[Graphs](#)

Branch: `master`

[Switch Branches \(1\)](#)

[Switch Tags \(0\)](#)

[Branch List](#)

Shell libraries to help writing shell script — [Read more](#)

[click here to add a homepage](#)

[Downloads](#)

SSH

HTTP

Git Read-Only

`git@github.com: Tauop/ScriptHelper.git`



This URL has **Read+Write** access

Display command when it's unknown



Tauop (author)

April 04, 2011

commit [29eaadb9851a3584b74f](#)

tree [77af569ed2c1baf211b3](#)

parent [025538739a5000a26048](#)

[ScriptHelper](#) /

name

age

message

[history](#)

IV. RÉUTILISATION DE SSHGATE

PARTICIPER AU DÉVELOPPEMENT

- ✓ SshGate : <http://www.github.com/Tauop/sshGate>
- ✓ ScriptHelper : <http://www.github.com/Tauop/ScriptHelper>
- ✓ Venez nous voir sur IRC@Freenode #linagora
- ✓ Contact : pguiran@linagora.com

Questions ?

MERCI DE VOTRE ATTENTION

Contact :

LINAGORA – Siège social

80, rue Roque de Fillol

92800 PUTEAUX

FRANCE

Tél. : 0 810 251 251 (tarif local)

Fax : +33 (0)1 46 96 63 64

Mail : info@linagora.comWeb : www.linagora.com