Distribution EOLE - Scénario #28576

Pouvoir logger les commandes utilisateurs

11/06/2019 15:02 - Emmanuel GARETTE

Statut:	Nouveau	**Début:**	
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure

Description

Besoins

- avec une information de "contexte" donnée par l'utilisateur (l'utilisateur doit pouvoir expliquer pourquoi il se connecte) ;
- savoir qui a exécuté les commandes (dans le cadre de Zéphir tout le monde se connecte en root), il faut trouver quelle clef SSH est utilisée ;
- savoir qui a exécuté la commande via sudo ;
- avoir un fichier unique des logs d'historiques de tous les utilisateurs connectés sur une machine ;
- que soit logger les commandes même si l'utilisateur faire : ssh xxxx@yyyyy nom_de_la_commande ;
- avoir le répertoire courant de l'exécution de la commande ;
- avoir un historique complet de la session (les commandes exécutées ainsi que les retours).

Exemple d'utilisation

Connexion utilisateur et exécution d'une commande via sudo

```
$ ssh xxx@yyyyy
Raison de la connection sur ce serveur : Intervention sur le serveur suite à problème de place

xxx@yyyyy $ sudo du -h -d1 /
[sudo] Mot de passe de xxx :
[..]
xxx@yyyyy $
```

Contenu des logs :

```
2019-06-11T14:37:57.455302+02:00 yyyyy history: "xxx" "xxx" "10.10.10.3 48752 22" "/home/xxx/.scre
en_history/session_24850_1560256625" "/dev/pts/3" "24908" "/home/xxx" "echo "*** Intervention sur
le serveur suite à problème de place ***""
2019-06-11T14:38:08.410720+02:00 yyyyy history: "xxx" "xxx" "10.10.10.3 48752 22" "/home/xxx/.scre
en_history/session_24850_1560256625" "/dev/pts/3" "24908" "/home/xxx" "sudo du -h -d1 /"
```

Explication des lignes :

Heure/date de la commande : 2019-06-11T14:37:57.455302+02:00
Nom de la machine : yyyyy
Nom du log : history:
Utilisateur qui a lancé la commande : xxx
Utilisateur déduit : xxx
Source (adresse ip source + port source + port de destination) : "10.10.10.3 48752 22"
Fichier d'enregistrement de la session : /home/xxx/.screen_history/session_24850_1560256625
TTY : /dev/pts/3
PPID : 24908
Répertoire d'exécution : /home/xxx
Commande : sudo du -h -d1 /

Contenu de /home/xxx/.screen_history/session_24850_1560256625 :

```
Raison de la connection sur ce serveur : Intervention sur le serveur suite à problème de place

xxx@yyyyy $ sudo du -h -d1 /
[sudo] Mot de passe de xxx :
[..]
xxx@yyyyy $
```

sudo -i + exécution d'une commande

```
2019-06-11T14:47:47.934138+02:00 yyyyy history: "xxx" "xxx" "10.10.10.3 48752 22" "/home/xxx/.screen_history/session_24850_1560256625" "/dev/pts/3" "24908" "/home/xxx" "sudo -i"
2019-06-11T14:47:51.894436+02:00 yyyyy history: "root" "xxx" "" "" "/dev/pts/3" "25179" "/root" "du -h -d1 /"
```

Connexion direct en root avec clef SSH (cas Zéphir) sans log de session

```
$ ssh root@yyyyy
root@yyyyy $ du -h -d1 /
[..]
```

Contenu du log :

```
2019-06-11T14:51:32.444218+02:00 yyyyy history: "xxx" "xxx@yyy.com" "10.10.10.3 48922 22" "" "/dev/pts/0" "25333" "/root" "du -h -d1 /"
```

exécuter de commande directement depuis la commande ssh

```
$ ssh xxx@yyyyy "du -h -d1 /"
[..]
```

Contenu du log :

```
2019-06-11T14:54:23.299933+02:00 yyyyy history: "xxx" "xxx" "10.10.10.3 48966 22" "" "pas un tty" "25539" "/home/xxx" "du -h -d1 /"
```

Historique

#1 - 11/06/2019 15:02 - Emmanuel GARETTE

- Fichier log.sh ajouté

#2 - 11/06/2019 15:03 - Emmanuel GARETTE

- Fichier screenrc ajouté

#3 - 11/06/2019 15:03 - Emmanuel GARETTE

- Fichier log.sh supprimé

#4 - 11/06/2019 15:06 - Emmanuel GARETTE

- Fichier bash.bashrc ajouté

- Fichier 00_loghistory.xml ajouté

- Fichier bashrc ajouté

#5 - 11/06/2019 15:13 - Emmanuel GARETTE

Le fonctionnement :

- pour les utilisateurs concernés pas l'enregistrement de la session doivent avoir le fichier .bashrc dans leur HOME ;
- un screen est exécuté a la connexion est enregistre les sessions ;
- les utilisateurs sans le .bashrc ont leur commande qui remonte dans les logs mais n'ont pas de session enregistrée.

#6 - 10/12/2021 15:06 - Gilles Grandgérard

- Tracker changé de Demande à Scénario

- Début 11/06/2019 supprimé

Fichiers

log.sh	1,72 ko	11/06/2019	Emmanuel GARETTE
screenrc	3,64 ko	11/06/2019	Emmanuel GARETTE
bash.bashrc	2,34 ko	11/06/2019	Emmanuel GARETTE
00_loghistory.xml	160 octets	11/06/2019	Emmanuel GARETTE
bashrc	430 octets	11/06/2019	Emmanuel GARETTE