

Distribution EOLE - Scénario #13335

Définir une configuration SSH sécurisée et utilisable avant instance

02/10/2015 10:48 - Philippe Caseiro

Statut:	Partiellement Réalisé	Début:	07/01/2016
Priorité:	Normal	Echéance:	22/01/2016
Assigné à:		% réalisé:	100%
Catégorie:		Temps estimé:	0.00 heure
Version cible:	sprint 2016 01-03 - Equipe MENESR	Temps passé:	10.58 heures

Description

Exigence

- Le serveur SSH doit autoriser la connexion au compte **root** avant l'instance
- Le compte utilisateur **root** doit avoir un mot de passe aléatoire avant l'instanciation
- Le compte utilisateur **eole** doit avoir un mot de passe aléatoire avant l'instanciation
- La transformation d'un serveur Ubuntu en module EOLE ne doit pas changer le mot de passe **root** si ce n'est pas celui par défaut d'EOLE

Proposition

Générer des mots de passe aléatoires dès l'installation de l'image ISO pour les comptes **root** et **eole**.

Tâches :

- Nécessite de modifier l'affichage du mot de passe sur la console physique. Le fichier est actuellement modifié par le **postinst** du paquet **eole-server** (eole-common:source:debian/eole-server.postinst@e618e4d#L89)
- Nécessite de modifier la procédure de changement de mot de passe à l'instanciation. Actuellement nous vérifions que le mot de passe actuel a bien été changé

Contraintes

- Nécessite un accès physique au serveur pour transmettre le mot de passe à l'utilisateur distant voulant se connecter en SSH

Contournement pour la 2.5.0 et la 2.5.1

1. Se connecter avec le compte **eole** et son mot de passe par défaut **\$fpmf&123456\$**
2. Passer **root** avec la commande **su** - et le mot de passe par défaut de **root \$eole&123456\$**
3. Modifier la configuration du serveur SSH

```
root@eolebase:~# sed -i -E 's,^(PermitRootLogin).*,\1 yes,' /etc/ssh/sshd_config
```

4. Redémarrer le serveur SSH

```
root@eolebase:~# service ssh restart
```

Demande utilisateur

En version 2.5 il est impossible d'ouvrir une session SSH avec l'utilisateur root. Ce qui en soit n'est pas un problème mais ce n'est pas dénué de conséquences.

Il est désormais impossible de configurer un serveur via SSH avant l'instance.

Pour lancer gen_config avant l'instance il faut :

1. Ouvrir une session avec le compte eole (seul compte disponible) et choisir "Shell_Linux" dans le menu.

2. Devenir root avec la commande "su -" eole n'a pas de droits "sudo"
3. Lancer gen_config une fois root.

Le problème est que gen_config ne se lance pas car il n'a pas le droit d'ouvrir le display forwarder.

Conclusion: en 2.5 il est impossible de configurer un serveur via SSH.

Sous-tâches:

Tâche # 14566: Ne plus mettre à jour le fichier issue dans le paquet eole-server	Ne sera pas résolu
Tâche # 14661: Créer l'utilisateur « eole » s'il n'existe pas	Fermé
Tâche # 14653: Ne pas définir de mot de passe aléatoire si le mot de passe courant n'es...	Fermé
Tâche # 14645: Gérer le changement de mot de passe durant la phase instance	Fermé
Tâche # 14567: Autoriser les connexions root dès l'installation ISO	Fermé
Tâche # 14565: Générer des mots de passe aléatoires à l'installation ISO	Fermé
Tâche # 14633: Infra EOLE: Modifier le mot de passe root avant le redémarrage	Fermé
Tâche # 14643: Exigences et tests squash	Reporté
Tâche # 14644: Mettre à jour la documentation d'installation	Fermé

Demandes liées:

Lié à eole-common - Bac à idée #12123: Chaque administrateur doit avoir un co... Nouveau

Historique

#1 - 02/11/2015 11:34 - Scrum Master

- Tracker changé de Anomalie à Demande

#2 - 02/11/2015 12:01 - Thierry Bertrand

Cela va nous poser problème au niveau de l'assistance au niveau de l'installation initiale.

Ne pourrait-on pas générer un mdp aléatoire pour root et l'afficher en console pour permettre à nouveau un accès ssh dès l'installation ?

#3 - 02/11/2015 12:06 - Scrum Master

- Assigné à mis à Daniel Dehennin

#4 - 10/11/2015 15:55 - Daniel Dehennin

Sur Ubuntu Trusty, seul la connexion par clef publique est autorisée pour le compte root et c'est cette configuration qui est en place avant l'instanciation du serveur.

Il existe plusieurs possibilités en fonction du niveau de sécurité voulue.

Serveur SSH non démarré avant instance

- Aucune connexion SSH n'est possible par défaut
- Cette option nécessite soit
 - de faire la configuration et l'instanciation en locale, physiquement devant le serveur
 - de faire configurer manuellement le service SSH et le démarrer pour une configuration et instanciation à distance

Il est aussi possible de :

- pré-configurer SSH pour autoriser des connexions avec les mots de passe par défaut
- générer des mots de passe aléatoires

Dans ce cas seul le démarrage manuel du service et la transmission éventuelle du mot de passe est nécessaire à la prise en main à distance.

Serveurs SSH démarré avant l'instance

- Cette option est le choix historique du projet EOLE.
- Plusieurs options sont envisageables dans ce mode de fonctionnement

Autoriser des connexions avec les mots de passe par défaut

- Permet de se connecter en SSH avec mot de passe pour les comptes **root** et **eole**
- Ouvre une fenêtre où le serveur peut être exploité par un mal veillant

Générer des mots de passe aléatoires dès l'installation de l'image ISO

- Nécessite l'affichage du mot de passe aléatoire sur la console physique, comme c'est actuellement le cas avec le mot de passe par défaut
- Nécessite de modifier la procédure de changement de mot de passe à l'instanciation
- Nécessite un accès physique au serveur pour transmettre le mot de passe à l'utilisateur distant voulant se connecter en SSH

#5 - 12/11/2015 10:48 - Scrum Master

Solution de mot de passe aléatoire retenue par le product owner pour la 2.5.2.

#6 - 12/11/2015 11:49 - Daniel Dehennin

- Tracker changé de Demande à Proposition Scénario

- Sujet changé de SSH, gen_config et 2.5 avant instance à Définir une configuration SSH sécurisée et utilisable avant instance

- Description mis à jour

- Assigné à Daniel Dehennin supprimé

#7 - 12/11/2015 11:50 - Daniel Dehennin

- Description mis à jour

#8 - 17/11/2015 15:54 - Scrum Master

- Tracker changé de Proposition Scénario à Scénario

- Début 02/10/2015 supprimé

- Release mis à EOLE 2.5.2

- Points de scénarios mis à 3.0

#9 - 16/12/2015 10:54 - Luc Bourdot

- Echéance mis à 22/01/2016

- Version cible mis à sprint 2016 01-03 - Equipe MENESR

- Début mis à 21/12/2015

#10 - 15/01/2016 15:04 - Daniel Dehennin

Amélioration de la formalisation des tâches :

- Ajout des procédures de validation

#11 - 15/01/2016 15:25 - Daniel Dehennin

- Description mis à jour

#12 - 26/01/2016 17:28 - Daniel Dehennin

- Statut changé de Nouveau à Partiellement Réalisé

#13 - 03/03/2016 09:10 - Daniel Dehennin

ERRATA

Pour les modules EOLE 2.5.0 et 2.5.1, la connexion avec le compte **root** n'est pas possible avant instance.

Pour contourner:

1. Se connecter avec le compte **eole** et son mot de passe par défaut **\$fpmf&123456\$**
2. Passer **root** avec la commande **su -** et le mot de passe par défaut de **root \$eole&123456\$**
3. Modifier la configuration du serveur SSH

```
root@eolebase:~# sed -i -E 's,^(PermitRootLogin).*,\1 yes,' /etc/ssh/sshd_config
```

4. Redémarrer le serveur SSH

```
root@eolebase:~# service ssh restart
```