Distribution EOLE - Tâche #33994

Scénario # 33908 (Terminé (Sprint)): EOLE 2.9 : Openssh 8.9

Etude

31/03/2022 14:15 - Emmanuel GARETTE

Statut:	Fermé	**Début:**	31/03/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Emmanuel GARETTE	**% réalisé:**	100%
Version cible:	Prestation Cadoles MEN 2022 13-15	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Vérifier les dépôts en plus de ceux du scénario :

```
scribe-ad/scripts/eolead:[ ! -f /root/.ssh/id_rsa.pub ] && ssh-keygen -f /root/.ssh/id_rsa -N ''
eole-common/lxc-templates/lxc-eole:        ssh-keygen -f "$auth_key" -N ''
eole-pacemaker/postservice/00-haute-dispo:            ssh-keygen -t rsa -b 2048 -f /root/.ssh/id_r
sa -N "" -q
eole-ad-dc/lib/eole/samba4.sh:        ssh-keygen -b 2048 -t rsa -f /root/.ssh/id_rsa -q -N ""
zephir-client/bin/enregistrement_zephir:    cmd = ['/usr/bin/ssh-keygen', '-N', '', '-b', '1024',
'-t', 'rsa', '-f', '/var/spool/uucp/.ssh/id_rsa', '-C', '"uucp@%s"' % adresse_zephir]
zephir-client/bin/enregistrement_zephir:        # erreur de la commande ssh-keygen
zephir-parc/python/zephir/backend/lib_backend.py:        res = os.system("""/usr/bin/ssh-keygen -N
 "" -b 1024 -t rsa -f %s -C uucp@%s""" % (new_key, zephir
```

Historique

#1 - 31/03/2022 14:15 - Emmanuel GARETTE

- Statut changé de Nouveau à En cours

- Assigné à mis à Emmanuel GARETTE

#2 - 31/03/2022 14:17 - Emmanuel GARETTE

J'ai trouvé en plus :

```
eole-hapy-deployment/scripts/deploy-auto:    fic_cle = open("/var/spool/uucp/.ssh/id_rsa.pub", "r")
eole-one-master/scripts/onehost_create_all:    REMOTEKEY=$(su - oneadmin -c "ssh ${host} 'cat ~oneadmin/.ssh/i
d_rsa.pub'")
zephir-client/data/scripts/update_key.zephir:        os.system("/bin/chown uucp.uucp %s/id_rsa*" % ssh_dir)
zephir-client/zephir/lib_zephir.py:    os.system("/bin/chown uucp.uucp %s/id_rsa*" % ssh_dir)
```

#3 - 31/03/2022 14:56 - Emmanuel GARETTE

D'après (entre autre) https://www.ssh-audit.com/ :

- ssh-dsa : à éviter
- ssh-rsa/SHA-1 : à éviter
- ssh-rsa/SHA-2 : OK
- ECDSA : très critiqué par certains spécialistes de la sécurité (NSA inside)
- Ed25519 : clef plus petites mais aussi sécurisées que leurs ancêtres, ce qui prend moins de ressources pour chiffrer et déchiffrer

Choix : Ed25519

#4 - 11/04/2022 10:04 - Emmanuel GARETTE

- Statut changé de En cours à À valider

- % réalisé changé de 0 à 100

#5 - 14/04/2022 15:35 - Benjamin Bohard

- Statut changé de À valider à Résolu

#6 - 15/04/2022 14:03 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0