Admins - Anomalie #1144

gestion des utilisateurs pour l'integration continue

22/12/2012 17:27 - Loïc Dachary

Statut:	Fermé	**Début:**	22/12/2012
Priorité:	Immédiate	**Echéance:**	
Assigné à:	François Poulain	**% réalisé:**	0%
Catégorie:	Task	**Temps estimé:**	0.00 heure
Version cible:	Backlog	**Temps passé:**	1.00 heure
Difficulté:	2 Facile		

Description

- faire un user sur ci.april.org et lui faire un bashrc qui charge les credentials openstack
- ajouter la clé dans toutes les vm déployées a des fins de test

Demandes liées:

Lié à Admins - Demande #1103: beta test de l'accueil des bénévoles	**Fermé**	**17/12/2012**
Lié à Admins - Demande #240: Mise en place d'un annuaire LDAP au sein du SI d...	**Fermé**	**31/12/2010**

Historique

#1 - 27/12/2012 00:27 - Loïc Dachary

- http://www.craigdunn.org/2011/03/puppet-working-with-define-based-virtuals/

#2 - 27/12/2012 00:29 - Loïc Dachary

- Statut changé de Confirmé à En cours de traitement

#3 - 27/12/2012 12:18 - Loïc Dachary

```
(11:17:14 AM) _aeris_: oui dachary ?
(11:17:26 AM) dachary: tu connais ldap ?
(11:17:34 AM) dachary: je ne connais pas ldap
(11:17:35 AM) _aeris_: un chouia
(11:17:45 AM) dachary: j'ai pas trop envie d'apprendre
(11:17:52 AM) _aeris_: je te confirme :D
(11:17:56 AM) dachary: mais la question mérite d'être posée
(11:18:00 AM) _aeris_: c'est juste imbouffable LDAP :D
(11:18:18 AM) dachary: parceque c'est supporté par openstack, jenkins, gerrit, redmine nativement
(11:18:43 AM) _aeris_: c'est sensé faire le café
(11:18:45 AM) _aeris_: mais c'est généralement assez compliqué à mettre en œuvre
(11:18:47 AM) dachary: _aeris_: comment tu ferais pour gérer un sso sans ldap ?
(11:18:52 AM) _aeris_: et en plus rien n'y est normalisé
(11:19:07 AM) _aeris_: avec ou sans ldap, ça ne change pas grand chose
(11:19:16 AM) _aeris_: le ldap ne sert qu'à stocker les mots de passe
(11:19:30 AM) dachary: je change ma question
(11:20:01 AM) dachary: comment tu fais pour éviter de définir plusieurs fois un user ( redmine, jenkins, gerri
t, openstack, etc.)
(11:20:03 AM) dachary: ?
(11:20:25 AM) _aeris_: ben là comme ça, je dirais LDAP
(11:20:33 AM) _aeris_: mais c'est pas gagné que ça soit si simple
(11:20:43 AM) vincentxavier: saylebien ldap
(11:20:50 AM) dachary: vincentxavier: tu connais ?
(11:20:57 AM) vincentxavier: oui pas trop mal
(11:21:01 AM) _aeris_: par exemple le ldap attendu par jenkins n'est clairement pas de la même structure que c
elle attendu par redmine
(11:21:09 AM) Sp4rKy: je dirais ldap aussi
(11:21:18 AM) dachary: s'il y a 2 personnes qui connaissent alors on va sérieusement devoir considerer la ques
tion
(11:21:24 AM) Sp4rKy: euh redmine tu peux définir les différents champs
(11:21:24 AM) dachary: Sp4rKy: tu connais aussi ?
(11:21:31 AM) Sp4rKy: dachary: oui, pas trop mal
(11:21:35 AM) _aeris_: y'a rien de normalisé, tout le monde utilise les schémas qui leurs plaisent
(11:21:40 AM) vincentxavier: le seul truc chiant pour l'instant àmha, c'est que gDTC ne connait pas LDAP
(11:21:56 AM) Sp4rKy: _aeris_: euhh, les inetorgperson etc... sont bien utilisés quand meme
```

(11:22:11 AM) _aeris_: ça doit être la seule chose bien utilisée :D
(11:22:16 AM) _aeris_: regarde les group…
(11:22:17 AM) Sp4rKy: :)
(11:22:19 AM) dachary: vincentxavier: quel que soit la solution retenue il y aura des sous systèmes qui ne le connaissent pas ou qui posent problème
(11:22:20 AM) vincentxavier: _aeris_: en pratique non, tu prends le inetOrgPerson et tu as yn gros dénominateur commun
(11:22:35 AM) Sp4rKy: on utilise au taf, avec répli, et connection sur un mediawiki, redmine, jenkins
(11:22:41 AM) _aeris_: oui, mais là ça ne fait que de l'authentification simple
(11:22:49 AM) Sp4rKy: donc au moins pour ces 3 là, ça marche pas trop mal :D
(11:22:49 AM) vincentxavier: dachary: oui, oui, et je pense que LDAP est la solution qui minimise le nombre de sous-sytème qui ne connaissent pas ldap
(11:22:54 AM) _aeris_: pas de gestion de droits ou de groupes par exemple
(11:22:58 AM) Sp4rKy: (+ appli persos)
(11:23:09 AM) ***dachary soupire et se résigne a apprendre ldap
(11:23:13 AM) vincentxavier: d'ailleurs sympa aussi connait ldap
(11:23:20 AM) vincentxavier: enfin, je dis ça, je dis rien
(11:23:27 AM) _aeris_: y'a pas mal de chose qui connais ldap oui
(11:23:39 AM) _aeris_: après, faut juste arriver à le mettre en place et que tout fonctionne
(11:24:10 AM) _aeris_: et si on parle redmine par exemple, ça veut dire que toute personne qui n'est pas dans le ldap ne peut pas se logguer
(11:24:15 AM) Sp4rKy: c'est probablement le backend le plus utilisé pour du partage de compte oui :)
(11:24:20 AM) vincentxavier: et puis depuis ldap 2.4 et la configuration stockée sous la forme d'un arbre ldap, c'est assez cool je trouve
(11:24:27 AM) vincentxavier: _aeris_: nope
(11:24:30 AM) _aeris_: je ne sais pas comment est fait l'authent sur le redmine actuellement
(11:24:40 AM) vincentxavier: _aeris_: pour redmine tu peux mélanger les authentifications
(11:24:44 AM) _aeris_: vx > euh, le config.d, on repassera quand même :d
(11:25:00 AM) _aeris_: c'est un peu la misère, et terriblement non documenté…
(11:25:00 AM) dachary: avec la gestion de configuration via puppet on a deux choix : ldap ou bien des modules puppet qui fabriquent des utilisateurs pour chaque sous système. J'ai une préférence pour la deuxième solution mais je pense que c'est un use case vraiment rare et qu'on serait les seuls a s'y aventurer.
(11:25:07 AM) vincentxavier: _aeris_: non, c'est ultime
(11:25:22 AM) _aeris_: ben si t'as une recette magique, je prend :D
(11:25:24 AM) vincentxavier: han puppet connait ldap aussi
(11:25:36 AM) Sp4rKy: oui
(11:25:38 AM) _aeris_: le jour où j'ai voulu activer ssl sur mon ldap, juste j'en ai chié
(11:25:40 AM) Sp4rKy: tu peux l'utiliser en backen
(11:26:27 AM) dachary: Sp4rKy: tu as déjà stocké les clés publiques ssh dans ldap ?
(11:26:36 AM) _aeris_: et un truc qui s'auto-utilise pour stocker sa conf, tu sents bien que la misère peu vite arriver :D
(11:26:37 AM) Sp4rKy: on fait ça oui
(11:26:45 AM) Sp4rKy: les users mettent leurs clés via un "portail"
(11:26:58 AM) Sp4rKy: et on les récup après via un script pour créer les comptes + clé sur un bastion ssh
(11:27:09 AM) Sp4rKy: (pas via puppet par contre)
(11:27:43 AM) dachary: Sp4rKy: et la clé est stocké dans un champ associé a l'utilisateur ?
(11:27:55 AM) dachary: (champ ldap)
(11:28:13 AM) Sp4rKy: oui
(11:28:18 AM) dachary: bon
(11:28:23 AM) Sp4rKy: dans un sshpublickey ou un truc comme ça
(11:28:35 AM) Sp4rKy: http://code.google.com/p/openssh-lpk/ ce schéma là
(11:29:00 AM) dachary: vincentxavier: tu as déjà utilisé redmine avec ldap en meme temps que la gestion des utilisateurs traditionelle ?
(11:29:13 AM) vincentxavier: oui
(11:29:31 AM) Sp4rKy: attention, on utilise pas le "patched openssh" , on stock juste les clés dans le ldap et on les rappatrie avec un script
(11:29:46 AM) Sp4rKy: te faut un ssh patché si tu veux utiliser ldap directement en backend ssh
(11:29:53 AM) dachary: Sp4rKy: compris
(11:30:10 AM) dachary: je pense que ce serait raisonable de
(11:30:17 AM) dachary: a) installer ldap
(11:30:30 AM) dachary: b) activer ldap sur le agir.april.org
(11:30:57 AM) dachary: c) configurer les *nouveaux* sous sytemes (openstack, gerrit, jenkins, puppet) pour utiliser ldap
(11:31:57 AM) dachary: d) définir un utilisateur dans puppet via ldap + via la methode non ldap si besoin (i.e. pour l'installation des cles ssh sur les machines)
(11:32:40 AM) Sp4rKy: "définir un utilisateur dans puppet via ldap" comment ça ?
(11:32:54 AM) Sp4rKy: attention, utiliser ldap en backend puppet, ça veut dire l'utiliser comme ENC de mémoire
(11:33:57 AM) dachary: hum
(11:34:18 AM) dachary: je pensais plus a backend de http://docs.puppetlabs.com/references/latest/type.html#user
(11:35:02 AM) Sp4rKy: dachary: je suis pas sur que tu puisses le faire sans configurer ldap globalement
(11:35:07 AM) Sp4rKy: pour tout puppet
(11:35:23 AM) dachary: ah
(11:36:05 AM) dachary: Sp4rKy: mais alors comment tu utilises la gestion des user dans puppet ? (hors le script qui install les clés ssh je veux dire)

(11:36:20 AM) dachary: votre ENC c'est ldap ?
(11:36:28 AM) Sp4rKy: non, notre enc c'est le dashboard
(11:36:34 AM) Sp4rKy: mais on l'utilise pas la gestion des users
(11:36:40 AM) Sp4rKy: enfin si, mais pour quelques users (les admins)
(11:36:47 AM) Sp4rKy: pas pour des centaines d'users
(11:36:54 AM) Sp4rKy: les users sont gérés dans le ldap
(11:36:57 AM) dachary: ok
(11:36:58 AM) Sp4rKy: mais indépendamment de puppet
(11:37:01 AM) dachary: ah !
(11:37:55 AM) ***dachary reflechit
(11:38:42 AM) Sp4rKy: attention ça fume
(11:39:53 AM) dachary: Sp4rKy: est-ce que tu as le cas ou puppet a besoin de faire un truc pour tous les utilisateurs ? Ou bien puppet reste totalement ignorant de la liste des utilisateurs ?
(11:40:15 AM) _aeris_: j'y go moi
(11:40:16 AM) _aeris_: @++
(11:40:21 AM) dachary: _aeris_: a+ !
(11:44:23 AM) Sp4rKy: dachary: en général il reste indépendant de la liste
(11:44:28 AM) Sp4rKy: tu penses à quoi comme cas ?
(11:51:43 AM) dachary: Sp4rKy: je n'ai pas de cas en tete
(11:52:55 AM) Sp4rKy: :)
(11:54:03 AM) dachary: ca me dérange d'avoir d'un coté une gestion de configuration centralisée et de l'autre une gestion d'utilisateur centralisée et que ce soit deux systèmes qui n'ont aucune interaction. Je pense que le script qui installe les cles ssh sur ton bastion est un exemple du problème que ça pose.
(11:54:25 AM) dachary: Sp4rKy: ce script est lancé par puppet ?
(11:55:03 AM) Sp4rKy: il est installé par puppet
(11:55:06 AM) Sp4rKy: et lancé par un cron
(11:55:11 AM) dachary: ok
(11:55:22 AM) Sp4rKy: en fait ce script est là car il est utilisé par des infras également sans puppet
(11:55:26 AM) Sp4rKy: mais qui ont le ldap
(11:56:03 AM) dachary: mettre les utilisateurs dans puppet (versus ldap) pose un probleme difficile : si un nouvel utilisateur demande un compte, il va le faire via une interface qui ne parle pas a puppet (par exemple redmine) et il faudra un script custom pour injecter / controller ça dans puppet.
(11:56:09 AM) dachary: donc c'est pas terrible
(11:56:53 AM) dachary: Sp4rKy: mais si tu avais a installer les clés ssh sur un systeme qui a puppet, tu ferais comment ?
(11:57:10 AM) Sp4rKy: pour l'instant via mon script :F
(11:57:18 AM) dachary: ok
(11:57:20 AM) Sp4rKy: après, faut voir si tu peux utiliser le ldap que pour les user dans puppt
(11:57:22 AM) Sp4rKy: puppet*
(11:57:26 AM) dachary: c'est pas forcément un mauvais systeme
(11:57:35 AM) Sp4rKy: et meme dans ce cas je suis pas sur qu'il gère les clésssh
(11:57:49 AM) Sp4rKy: car le sshpublickey n'est pas un attribut "classique" dans ldap
(11:57:52 AM) dachary: Sp4rKy: effectivement il ne gere pas les clés ssh
(11:58:01 AM) dachary: j'ai rien vu dans ce sens
(11:58:31 AM) Sp4rKy: Sinon, si tu veux gérer ça vraiment via ldap, peut etre que utiliser hiera avec un backend ldap pourrait le faire
(11:59:08 AM) dachary: je le sens pas trop le couplage puppet ldap
(11:59:17 AM) Sp4rKy: mais idem, si tu te mets à utiliser hiera, en général tu l'utilises aussi comme enc
(11:59:25 AM) dachary: voila
(11:59:31 AM) dachary: on a un truc sans enc
(11:59:37 AM) Sp4rKy: pour l'instant
(11:59:55 AM) dachary: pour l'april ca devrait convenir pour plusieurs années
(12:00:07 PM) dachary: parceque l'infrastructure est petite et le restera
(12:00:09 PM) Sp4rKy: himo ce sont 2 choses différentes la base user et puppet, je suis pas sur que , meme si c'était possible, je gérerais mes users via puppet
(12:00:23 PM) Sp4rKy: ne serait ce que pour le temps que prendrait chaque run à vérifier tous les users
(12:00:27 PM) dachary: Sp4rKy: c'est aussi la conclusion a laquelle j'arrive
(12:00:45 PM) dachary: c'est pas vraiment fait pour
(12:00:50 PM) Sp4rKy: voila
(12:01:24 PM) dachary: il faut que puppet puisse consulter la base user (par exemple pour distribuer des clés) mais ça peut se faire via un script ou une fonction puppet si on veut faire smart et intégré
(12:01:31 PM) Sp4rKy: yep
(12:02:00 PM) Sp4rKy: pour l'instant sur l'infra ubuntu (pas de ldap cette fois) on a une entrée user et un file{} pour la clé ssh
(12:02:14 PM) dachary: ok
(12:02:22 PM) Sp4rKy: enfin un define ssh ()
(12:02:28 PM) Sp4rKy: qui fait 2/3 trucs, mais la partie importante est le file
(12:03:15 PM) Sp4rKy: et après on a des classes pour les cas "classqiesu"
(12:03:17 PM) dachary: supposons donc que l'utilisateur soit créé via gerrit (qui gere la clé ssh donc c'est un bon point d'entrée)
(12:03:18 PM) Sp4rKy: genre inclure les admins
(12:04:30 PM) dachary: Sp4rKy: comment tu gere les groupes ? i.e. un utilistateur a un compte admin dans redmine, il est simple utilisateur dans jenkins, sa clé ssh doit etre installé sur les machines de test et / ou les machines de prod ... ce genre de chose.
(12:05:35 PM) dachary: je devrais poser la question autrement

```
(12:05:48 PM) Sp4rKy: alors on a pas de gestion de groupes poussée
(12:06:01 PM) dachary: quand un utilisateur est créé, comment tu dis : c'est un user redmine et un user jenkin
s ( ou pas )
(12:06:11 PM) Sp4rKy: c'est par défaut un user partout de mémoire
(12:06:31 PM) Sp4rKy: première fois qu'il va se logguer sur redmine, il aura ses infos rapatriées du ldap
(12:06:44 PM) Sp4rKy: pour jenkins, je m'occupe pas trop de cette partie, mais de mémoire c'est +/- le meme sy
stème
(12:07:02 PM) dachary: donc par défaut l'utilisateur existe partout
(12:07:08 PM) Sp4rKy: oui
(12:07:11 PM) dachary: ou nulle part
(12:07:11 PM) Sp4rKy: c'est le but du ldap quoi :}
(12:07:16 PM) Sp4rKy: pour ce qui est des machines de dev/prod, on a 3 classes puppet pour ça
(12:07:22 PM) Sp4rKy: admins, dev, dev-ro
(12:07:30 PM) dachary: ah
(12:07:32 PM) Sp4rKy: chacune crée les comptes qui vont bien sur les machines
(12:07:40 PM) Sp4rKy: enfin non
(12:07:45 PM) Sp4rKy: enfin si ...
(12:07:48 PM) dachary: ahah
(12:07:49 PM) dachary: :-D
(12:07:51 PM) Sp4rKy: on a un compte d'admin partagé :D
(12:08:03 PM) Sp4rKy: donc les comptes = foo-admin ou foo-dev
(12:08:04 PM) dachary: créé via user {} de puppet ?
(12:08:31 PM) Sp4rKy: yes
(12:08:37 PM) Sp4rKy: on crée le user via user {}
(12:08:54 PM) Sp4rKy: on fout le ssh/config ssh/authorized_keys .bashrc via file {}
(12:09:29 PM) Sp4rKy: en fait le authorized_keys exporte une variable d'env, reprise dans le bashrc
(12:09:42 PM) Sp4rKy: qui permet d'avoir dans les logs "intel s'est connecté via foo-admin"
(12:10:23 PM) Sp4rKy: pour l'instant on a que 1 authorized_keys par user
(12:10:45 PM) Sp4rKy: mais c'est déja prévu pour utiliser concat{} et donc éventuellement en concaténer plusie
urs
(12:11:04 PM) Sp4rKy: (on pourrait par exemple imaginer avoir un @@concat::fragment pour chaque user
(12:11:14 PM) Sp4rKy: taggué avec un truc style tag => admin ou tag => dev
(12:11:27 PM) Sp4rKy: et faire un collect la dessus pluptot que d'avoir un fichier global
(12:11:29 PM) Sp4rKy: bref
(12:11:40 PM) Sp4rKy: et donc, ensuite, suivant qu'on inclu une ou 2 des 3 classes
(12:11:45 PM) Sp4rKy: y'a un compte admin, avec sudo total
(12:11:51 PM) Sp4rKy: un compte dev (pour l'inté) avec sudo total
(12:12:08 PM) Sp4rKy: et un compte dev-ro, qui permet aux devs d'avoir un accès read only aux logs et au sql d
e prod
(12:12:24 PM) Sp4rKy: </pavé>
(12:12:31 PM) dachary: donc en fait tu gère les comptes traditionels ( /etc/passwd ;-) via puppet et le reste
via ldap
(12:13:07 PM) dachary: il faut peut etre que j'arrete de penser unifier la gestion de tous les users
```

#4 - 04/01/2013 17:54 - Loïc Dachary

- Priorité changé de Normale à Immédiate

#5 - 04/01/2013 17:54 - Loïc Dachary

- Version cible changé de Décembre 2012 (2/2) à Backlog

#6 - 20/07/2014 22:43 - Vincent-Xavier JUMEL

- Statut changé de En cours de traitement à Un jour peut-être

- Assigné à Loïc Dachary supprimé

#7 - 20/10/2016 13:57 - François Poulain

- Description mis à jour

- Statut changé de Un jour peut-être à Fermé

Concerne des techno abandonnées.

#8 - 26/12/2020 01:17 - Christian P. Momon

- Assigné à mis à François Poulain