eole-common - Bac à idée #10803

La centralisation des journaux doit séparer les journaux de serveurs différents venant d'une même adresse ip (NAT)

06/03/2015 13:10 - Karim Ayari

Statut:	Nouveau	**Début:**	19/09/2014
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure

Description

Exigence

Les journaux des serveurs partageant la même adresse IP doivent être différenciés

Demande utilisateur initiale

si plusieurs serveurs derrière une même adresse ip sont configurés pour envoyer les logs,
côté serveur de réception les logs sont tous mélangés. il n'y a pas de différenciation des serveurs.

pour cela j'ai patché le template rsyslog_templates.conf que j'ai joint à la demande pour ajouter un répertoire supplémentaire basé sur le nom du serveur client avec la variable **%hostname%**

je me suis également rendu compte que certains services utilisent leur propre fichier de configuration rsyslog et de ce fait ne sont également pas répertorié par serveur. C'est le cas pour cron, iptables, auth et rsyslog.

```
rsyslog_traps_cron.conf.patch
rsyslog_traps_iptables.conf.patch
rsyslog_views_auth.conf.patch
rsyslog_traps_rsyslog.conf.patch
```

au final on se retrouve avec l'arborescence suivante :

```
remote/
├── adresse_ip_1
│   ├── serveur1
│   │   ├── service1
│   │   │   ├──
│   │   ├── service2
│   │   │   └──
│   └── serveur2
│   │   ├── service1
│   │   │   ├──
│   │   ├── service2
│   │   │   └──
└── adresse_ip_2
│   ├── serveur1
│   │   ├── service1
│   │   │   ├──
│   │   ├── service2
│   │   │   └──
│   └── serveur2
│   │   ├── service1
│   │   │   ├──
```

Sous-tâches:

Tâche # 8482: arborescence dans zephir par ID et par par IP **Nouveau**

Historique

#1 - 02/11/2015 14:44 - Joël Cuissinat

- Tracker changé de Evolution à Tâche

- Temps estimé mis à 4.00 h

- Tâche parente mis à #8550

- Restant à faire (heures) mis à 4.0

#2 - 18/11/2015 16:04 - Daniel Dehennin

- Tracker changé de Tâche à Proposition Scénario

- Sujet changé de serveur de logs: séparer les logs des serveurs venant d'une même adresse ip à La centralisation des journaux doit séparer les journaux de serveurs différents venant d'une même adresse ip (NAT)

- Description mis à jour

- Temps estimé 4.00 h supprimé

- Tâche parente #8550 supprimé

#3 - 18/11/2015 17:35 - Daniel Dehennin

- Projet changé de Distribution EOLE à eole-common

#4 - 27/11/2015 15:26 - Scrum Master

- Tracker changé de Proposition Scénario à Bac à idée

Fichiers

rsyslog_traps_cron.conf.patch	731 octets	06/03/2015	Karim Ayari
rsyslog_templates.conf.patch	519 octets	06/03/2015	Karim Ayari
rsyslog_traps_rsyslog.conf.patch	753 octets	06/03/2015	Karim Ayari
rsyslog_traps_iptables.conf.patch	715 octets	06/03/2015	Karim Ayari
rsyslog_views_auth.conf.patch	526 octets	06/03/2015	Karim Ayari