Distribution EOLE - Evolution #1204

Revoir la politique de journalisation des logs

18/11/2010 15:55 - Luc Bourdot

Statut:	Fermé	**Début:**	18/11/2010
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.50 heure
Distribution:	Toutes		

Description

Il faudrait mettre un garde-fou pour eviter la saturation du FileSystem /var/log

Demandes liées:

Lié à eole-exim - Anomalie #2517: exim4 : ne semble pas utiliser syslog	**Fermé**	**02/12/2011**	
Lié à eole-common - Anomalie #2432: rsyslog.logrotate n'est pas un template	**Fermé**	**18/11/2011**	
Lié à eole-proxy - Evolution #3018: Le fichier de configuration rsyslog de sq...	**Fermé**	**06/03/2012**	
Lié à zephir-client - Anomalie #2708: Gérer les logs des agents zéphir	**Fermé**	**12/01/2012**	
Lié à eole-common - Evolution #2563: separation des logs et la version de sca...	**Fermé**	**07/12/2011**	
Lié à zephir-client - Evolution #1492: Revoir la façon dont sont gérés les lo...	**Fermé**	**01/03/2011**	
Lié à ZéphirLog - Anomalie #1226: Ajouter la variable "activer_sonde_prelude"...	**Fermé**	**29/11/2010**	
Lié à ZéphirLog - Anomalie #794: ZephirLogs	**Pas un bug**	**23/07/2010**	
Lié à Amon - Anomalie #1348: log dansgardian	**Classée sans suite**	**12/01/2011**	
Lié à controle-vnc - Anomalie #2511: Log de controle-vnc non remonté sur le m...	**Fermé**	**02/12/2011**	
Lié à creole - Anomalie #660: parsedico log dans le logger "root"	**Ne sera pas résolu**	**11/06/2010**	
Lié à Documentations - Anomalie #372: Documenter ZephirLog	**Ne sera pas résolu**	**12/04/2010**	
Lié à eole-common - Anomalie #3161: [rsyslog] le port 20514 n'est pas accessi...	**Fermé**	**26/03/2012**	
Lié à Sentinelle - Anomalie #429: logs sentinelle	**Ne sera pas résolu**	**19/04/2010**	
Lié à eole-proxy - Anomalie #3066: règles distinctes de squid et iptables pou...	**Fermé**	**12/03/2012**	
Lié à conf-amon - Anomalie #3245: [logrotate] un template est fourni pour @/e...	**Fermé**	**05/04/2012**	
Lié à EoleSSO - Anomalie #3248: [log] N'utilise pas syslog	**Fermé**	**05/04/2012**	
Lié à courier-eolecas - Anomalie #3250: [log] Utilise syslog mais pas des fois	**Fermé**	**16/04/2012**	**19/07/2013**
Lié à ead - Anomalie #3271: Pas de virus dans l'observation des virus (ead)	**Fermé**	**11/04/2012**	
Lié à ead - Anomalie #3395: Plus d'historique de navigation Web dans L'EAD de...	**Fermé**	**25/04/2012**	
Lié à eole-proxy - Anomalie #3541: Mise à niveau du logrotate de dansguardian	**Fermé**	**30/05/2012**	
Lié à eole-common - Anomalie #3636: logrotate manquant à gérer dans le paquet...	**Fermé**	**15/06/2012**	
Lié à zephir-client - Anomalie #3646: logrotate manquant à gérer dans le paqu...	**Fermé**	**15/06/2012**	
Lié à eole-spamassassin - Anomalie #3645: logrotate manquant à gérer dans le ...	**Fermé**	**15/06/2012**	
Lié à eole-courier - Anomalie #3643: logrotate manquant à gérer dans le paque...	**Fermé**	**15/06/2012**	
Lié à EoleSSO - Anomalie #3642: logrotate manquant à gérer dans le paquet Eol...	**Fermé**	**15/06/2012**	
Lié à eole-dhcp - Anomalie #3641: logrotate manquant à gérer dans le paquet e...	**Fermé**	**15/06/2012**	
Lié à eole-web - Anomalie #3639: logrotate manquant à gérer dans le paquet eo...	**Fermé**	**15/06/2012**	
Lié à eole-proxy - Anomalie #3640: logrotate manquant à gérer dans le paquet ...	**Fermé**	**15/06/2012**	
Lié à conf-scribe - Anomalie #3638: logrotate manquant à gérer dans le paquet...	**Fermé**	**15/06/2012**	
Lié à eole-web - Demande #21035: Passer LogLevel de info à warn	**Ne sera pas résolu**	**11/07/2017**	

Révisions associées

Révision 118378f5 - 11/01/2009 01:07 - moyooo

see #1204 : Manage UTF8 filename

Révision 5439c58d - 21/03/2012 17:05 - Benjamin Bohard

refactoring des logs (ref #1204)

mise à jour de la référence au fichier de règles de ryslsog en mode
contexte de conteneur : 50-default.conf -> 00-aggregation.conf et
50-default-conteneur.conf -> 00-conteneur.conf
Modification de la configuration de apache2 : ErrorLog syslog et level
info

Révision f4ea601e - 21/03/2012 17:09 - Benjamin Bohard

refactoring log (ref #1204)

utilisation d'un template pour créer l'arborescence des journaux
dynamiquement.

Révision 7be43451 - 21/03/2012 17:35 - Benjamin Bohard

refactoring des logs (ref #1204)

Mise à jour de la référence au fichier de règle pour rsyslog en contexte
de conteneur : 50-default.conf -> 00-aggregation.conf et
50-default-conteneur.conf -> 00-conteneur.conf.
Répercussion du changement d'arborescence dans squid.logrotate.

Révision 7461f286 - 21/03/2012 17:40 - Benjamin Bohard

refactoring des logs (ref #1204)

Mise à jour des références au fichier de règles de rsyslog en contexte
de conteneur : 50-default.conf -> 00-aggregation.conf et
50-default-conteneur.conf -> 00-conteneur.conf

Révision f3876f4f - 21/03/2012 18:07 - Benjamin Bohard

refactoring de la gestion des logs (ref #1204)

modification en profondeur du dictionnaire dicos/01_log.xml :
- séparation des sources de logs selon le protocole ;
- mise à jour des fichiers à charger.
modification des fichiers de configuration :
- rsyslog.conf : chargement des modules complété (RELP, TCP et UDP si besoin),
correction du groupe cible pour l'abandon des droits root (problèmes
d'écriture dans /var/log/rsyslog même avec les bons droits) ;
- schéma général : /var/log/rsyslog/%hostname%/%programname%/%programname%.%syslogseverity-text% ;
- 00-aggregation.conf : prend en charge l'envoi par TCP (si TLS) ou
RELP ;
- 00-conteneur.conf : le seul fichier à placer dans un conteneur,
prévoit l'utilisation d'une file d'attente pour squid et une règle
générale pour le reste ;
- 20-... : filtres personnalisés pour certains programmes : squid, iptables,
ajout de rsyslog pour se conformer au schéma général (instances avec des
noms différents) ;
- 99-general_dispatch.conf : "ramasse-miettes", filtre tout le reste selon
le shéma général.
- rsyslog.logrotate : répercussion du changement d'arborescence pour

une partie des règles.

Révision 183b9683 - 21/03/2012 18:26 - Benjamin Bohard

refactoring des logs (ref #1204)

Mise à jour de la référence au fichier de règles de rsyslog en contexte
de conteneur : 50-default.conf -> 00-aggregation.conf et
50-default-conteneur.conf -> 00-conteneur.conf.
Ajout de la directive log_path_file = syslog dans le fichier de
configuration d'exim.
Répercussion du changement d'arborescence dans le fichier de logrotate.

Révision d6aed833 - 21/03/2012 18:55 - Benjamin Bohard

refactoring de la gestion des logs (ref #1204)

modification en profondeur du dictionnaire dicos/01_log.xml :
- séparation des sources de logs selon le protocole ;
- mise à jour des fichiers à charger.
modification des fichiers de configuration :
- rsyslog.conf : chargement des modules complété (RELP, TCP et UDP si besoin),
correction du groupe cible pour l'abandon des droits root (problèmes
d'écriture dans /var/log/rsyslog même avec les bons droits) ;
- schéma général : /var/log/rsyslog/%hostname%/%programname%/%programname%.%syslogseverity-text% ;
- 00-aggregation.conf : prend en charge l'envoi par TCP (si TLS) ou
RELP ;
- 00-conteneur.conf : le seul fichier à placer dans un conteneur,
prévoit l'utilisation d'une file d'attente pour squid et une règle
générale pour le reste ;
- 20-... : filtres personnalisés pour certains programmes : squid, iptables,
ajout de rsyslog pour se conformer au schéma général (instances avec des
noms différents) ;
- 99-general_dispatch.conf : "ramasse-miettes", filtre tout le reste selon
le shéma général.
- rsyslog.logrotate : répercussion du changement d'arborescence pour
une partie des règles.

Révision aeff92ab - 23/03/2012 16:32 - Benjamin Bohard

Les règles iptables bloquent les paquets entre conteneurs et root (ref #1204)

tmpl/end_static_rules.sh : ajout d'une règle autorisant les paquets tcp
sur le port 20514 depuis les conteneurs vers le maître.

Révision 0be8388e - 26/03/2012 17:54 - Benjamin Bohard

Corrections des paramètre TLS (ref #1204)

dicos/01_log.xml : réorganisation du dictionnaire pour la gestion de TLS
tmpl/00-aggregation.conf : réécriture du template pour la gestion de TLS
tmpl/rsyslog.conf : réécriture du template pour la gestion de TLS

Révision 2f9a50f2 - 30/03/2012 13:04 - Benjamin Bohard

migration de la journalisation de bacula (ref #1204)

syslog/20-bacula.conf : réécriture de la règle pour la nouvelle arborescence.
tmpl/bacula-common.logrotate : réécriture pour correspondre à la nouvelle arborescence.

Révision 3fd6fb1a - 30/03/2012 15:07 - Benjamin Bohard

mise en conformité de la gestion des logs (ref #1204)

rsyslog/20-named.conf : réécriture de la règle conformément à la nouvelle arborescence.
rvp/rsyslog/20-charon.conf : réécriture de la règle conformément à la nouvelle arborescence.
rvp/logrotate/charon : réécriture de la règle pour correspondre à la nouvelle arborescence.

Révision 28fa7dca - 30/03/2012 15:30 - Benjamin Bohard

mise à jour des configurations de journalisation (ref #1204)

rsyslog/20-nmbd.conf : réécriture de la règle pour se conformer à la nouvelle arborescence.
rsyslog/20-smbd.conf : réécriture de la règle pour se conformer à la nouvelle arborescence.
logrotate/smbd_nmbd : réécriture de la règle pour correspondre à la nouvelle arborescence.

Révision aabb2186 - 30/03/2012 15:44 - Benjamin Bohard

mise à jour des configurations de journalisation (ref #1204)

tmpl/20-squid.conf : réécriture de la règle pour se conformer à la nouvelle arborescence.
tmpl/99general-dispatch.conf : réécriture des règles pour se conformer à la nouvelle arborescence.
tmpl/rsyslog.logrotate : réécriture d'une partie des règles pour correspondre à la nouvelle arborescence.

Révision 50781435 - 30/03/2012 15:53 - Benjamin Bohard

correction des templates pour rsyslog (ref #1204)

- tmpl/99-general_dispatch.conf : il manquait .log à la fin et la variable syslogseverity-text à la place de syslogseverity.

Révision df29ebdc - 30/03/2012 16:23 - Benjamin Bohard

mise à jour de la configuration de journalisation (ref #1204)

- dansguardian*.conf : activation de l'option logsyslog (logsyslog = on plutôt que syslog = on).
- dansguardian.logrotate : réécriture de la règle pour correspondre à la nouvelle arborescence.
- squid.logrotate : réécriture de la règle pour correspondre à la nouvelle arborescence.

Révision a52d1fea - 30/03/2012 16:46 - Benjamin Bohard

mise à jour de la configuration pour la journalisation (ref #1204)

- tmpl/20-dansguardian.conf : ajout d'un fichier avec une règle pour rsyslog
- dicos/23_proxy.xml : ajout de l'entrée file prenant en charge le nouveau fichier 20-dansguardian.conf

Révision c316b257 - 30/03/2012 17:03 - Benjamin Bohard

correction de la journalisation d'iptables (ref #1204)

- tmpl/20-iptables.conf : correction du filtre
- tmpl/rsyslog.logrotate : ajout d'une règle pour iptables

Révision 9a0453e3 - 03/04/2012 18:48 - Benjamin Bohard

refactoring de l'arborescence générale des logs (ref #1204)

L'arborescence précédemment mise en place ne garantissait pas l'homogénéité entre le mode conteneur et le mode non conteneur. L'arborescence retenue pour cette itération est divisée en deux branches. La branche locale accueille les journaux locaux triés par programme (y compris conteneurs si utilisés). La branche remote accueille les journaux des machines distantes, triés par nom d'hôte puis par programme.

- 00-aggregation.conf : mise à jour pour conformité avec la nouvelle arborescence.

- 01-templates.conf : déport des templates génériques pour une éventuelle utilisation dans les règles personnalisées et, surtout, une meilleure identification.
- 20-auth.conf : création d'une règle de type "vue" pour amalgamer les messages concernant les authentifications (création de doublons).
- 80-rsyslog.conf : création d'une règle pour amalgamer les messages des différentes instances de rsyslog.
- 99-general_dispatch : mise à jour pour conformité avec la nouvelle arborescence et suppression des templates (voir 01-templates.conf).
- rsyslog.logrotate : mise à jour pour conformité avec la nouvelle arborescence.

Révision 15ff87dd - 05/04/2012 14:47 - Daniel Dehennin

Samba n'utilise pas syslog: Revert "mise à jour des configurations de journalisation (ref #1204)".

This reverts commit 28fa7dcae17f4c71559beac5bf71ccd35b5446cd.

Révision 599a0a2f - 05/04/2012 15:14 - Daniel Dehennin

Configuration de la rotation des logs de charon avec la nouvelle architecture.

- rvp/logrotate/charon: Les logs se trouvent dans /var/log/rsyslog/local/charon/

Ref: #1204 @5m

Révision cf8521f3 - 05/04/2012 15:39 - Benjamin Bohard

mise à jour du dictionnaire 01_log.xml (ref #1204)

Le dictionnaire installe les bons fichiers de configuration pour rsyslog.

Révision 7daf0041 - 10/04/2012 11:21 - Daniel Dehennin

Rsyslog: Ajout d'une règlè pour le trie des logs des conteneurs.

- tmpl/99-general_dispatch.conf: On utilise « :fromhost » en plus de « :fromhost-ip » du fait de problème avec la version rsyslog de Lucid.

Ref: #2871 @45m
Ref: #1204

Révision 6075242b - 23/05/2012 11:47 - Benjamin Bohard

problème de template rsyslog pour squid

- tmpl/00-aggregation.conf : ajout d'une condition sur les valeurs de %%squid_heure_debut et %%squid_heure_fin.
- tmpl/00-conteneur.conf : suppression de la condition sur %%activate_squide_tems_realtime.

Ref #1204

Révision fecdc38b - 25/05/2012 12:09 - Benjamin Bohard

Les templates ne permettent pas d'appliquer la politique de journalisation

- tmpl/80-squid.conf: règle de filtrage pour squid exploitant la différence de facility des instances.
- tmpl/80-dansguardian.conf: règle de filtrage pour dansguardian exploitant la différence de nom de programme des instances.
- dicos/23_proxy.xml: balise file pour 80-dansguardian.conf.
- tmpl/dansguardian1.conf: ajout de la variable "namesuffix" avec défaut à "$z"
- tmpl/dansguardian2.conf: ajout de la variable "namesuffix" avec défaut à "$z"
- tmpl/dansguardian3.conf: ajout de la variable "namesuffix" avec défaut à "$z"
- tmpl/squid.conf: utilisation de la facility LOG_LOCAL1
- tmpl/squid2.conf: utilisation de la facility LOG_LOCAL2

Ref #1204

Révision 57794e46 - 11/06/2012 09:41 - Benjamin Bohard

Correction du chemin des logs eole-sso pour logrotate

- logrotate/eole-sso : correction du chemin pour correspondre au nouveau dispatch.

Ref #1204

Révision a8b82850 - 11/06/2012 10:07 - Benjamin Bohard

Les répertoires créés avant l'abandon des privilèges sont inaccessibles après.

- tmpl/rsyslog.conf : ajout des directives $DirUser syslog et $DirGroup adm.

Ref #1204

Révision a120b623 - 13/06/2012 11:27 - Benjamin Bohard

Corrections des fichiers de conf de rsyslog.

- tmpl/80-cron.conf : copier/coller fâcheux, nom de template corrigé.
- tmpl/rsyslog.conf : correction de la directive $DirUser -> $DirOwner.

Ref #1204

Historique

#1 - 03/11/2011 10:38 - Joël Cuissinat

- Assigné à mis à Daniel Dehennin

#2 - 28/11/2011 10:14 - Daniel Dehennin

- Distribution mis à Toutes

Faire en sorte que tout passe par syslog, cf l'horreur de #1454.

#3 - 30/03/2012 12:08 - Joël Cuissinat

- Fichier logs.txt ajouté

Je joins mon rapport concernant les programmes qui vont fouiner (et des fois même écrire) dans les logs.
Demandes déjà rentrées :

- agent eximstats : #3213
- détection des virus : #3271 (ead) et #3400 (agent)
- observatoire de la navigation EAD : #3395

#4 - 10/04/2012 10:39 - Daniel Dehennin

Le filtrage avec :fromhost-ip ne semble fonctionner que pour les messages adressé à l'adresse IP de la carte eth0.

#5 - 10/04/2012 11:18 - Daniel Dehennin

Daniel Dehennin a écrit :

> Le filtrage avec :fromhost-ip ne semble fonctionner que pour les messages adressé à l'adresse IP de la carte eth0.

Mais cela ne fonctionne pas avec un rsyslog de Lucid :-/

#6 - 30/05/2012 10:46 - Daniel Dehennin

Il faut revoir les logrotate

```
root@amonecole:~# grep /var/log/rsyslog/ /etc/logrotate.d/*
/etc/logrotate.d/bacula-common:/var/log/rsyslog/local/bacula*/*.log {
/etc/logrotate.d/charon:/var/log/rsyslog/local/charon/*.log {
/etc/logrotate.d/eole-exim:/var/log/rsyslog/local/exim/*.alert.log {
/etc/logrotate.d/eole-exim:/var/log/rsyslog/local/exim/*.[!a]*.log {
/etc/logrotate.d/named:/var/log/rsyslog/local/named/*.log {
/etc/logrotate.d/rsyslog:/var/log/rsyslog/local/auth/*.log {
/etc/logrotate.d/rsyslog:/var/log/rsyslog/local/iptables/*.log {
/etc/logrotate.d/rsyslog:/var/log/rsyslog/local/CRON/*.log {
/etc/logrotate.d/rsyslog:/var/log/rsyslog/local/kernel/*.log {
/etc/logrotate.d/squid3:/var/log/rsyslog/local/squid/squid.info.log {
/etc/logrotate.d/squid3:/var/log/rsyslog/local/squid/squid.[!i]*.log
root@amonecole:~# ls -1 /var/log/rsyslog/local/
10freedos
10qnx
20microsoft
30utility
50mounted-tests
apache2
archived
archived.pl
auth
authdaemond
bastion
bounced
bounced.pl
charon
cron
CRON
dansguardian
dhclient
dhcpd
eolesso
exim
IMAP
imapd
init
ipsec_starter
kernel
login
macosx-prober
modprobe
named
ntpd
os-prober
pluto
proftpd
python
rngd
rsyslog
slapd
smbd
spamd
squid
sshd
sSMTP
su
sudo
sympa
task_manager
twisted
wwsympa
zephir
zephiragents
```

Voilà la liste des répertoires manquants, donc non géré par les logrotates.

```
10freedos
```

```
10qnx
20microsoft
30utility
50mounted-tests
apache2
archived
archived.pl
authdaemond
bastion
bounced
bounced.pl
cron
dansguardian
dhclient
dhcpd
eolesso
IMAP
imapd
init
ipsec_starter
login
macosx-prober
modprobe
ntpd
os-prober
pluto
proftpd
python
rngd
rsyslog
slapd
smbd
spamd
sshd
sSMTP
su
sudo
sympa
task_manager
twisted
wwsympa
zephir
zephiragents
```

#7 - 07/06/2012 10:24 - Benjamin Bohard

Il y a, en plus, des fichiers dans /var/log/ qui ne sont pas pris en charge par logrotate.

#8 - 07/11/2014 15:33 - Joël Cuissinat

- Statut changé de Nouveau à Fermé

- Assigné à Daniel Dehennin supprimé

- % réalisé changé de 0 à 100

#9 - 13/07/2017 17:32 - Joël Cuissinat

- Lié à Demande #21035: Passer LogLevel de info à warn ajouté

Fichiers

logs.txt	2,85 ko	30/03/2012	Joël Cuissinat