Distribution EOLE - Tâche #34772

Scénario # 34727 (Terminé (Sprint)): Gestion des logs générés par les applications installées dans les conteneurs podman

Étude

24/10/2022 12:16 - Benjamin Bohard

Statut:	Fermé	**Début:**	01/10/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Version cible:	Livraison Cadoles 30/11/2022	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 24/10/2022 12:16 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#2 - 24/10/2022 14:55 - Benjamin Bohard

Il existe une option permettant de modifier le nom du programme associé aux journaux. Malheureusement, la version embarquée sur Ubuntu (3.4.4 + quelques patchs) n'est pas fonctionnelle de ce point de vue :

- le nom du conteneur devrait normalement être utilisé à la place de conmon, ce qui ne nous arrangerait pas vu que ce nom est différent à chaque exécution ;
- l'option tag ne semble pas avoir d'effet ;
- les journaux sont en double (conmon + podman).

Testé avec succès avec la version 4.2.1 de podman sur une fedora pour vérifier (https://github.com/containers/podman/issues/13200).

#3 - 25/10/2022 09:42 - Benjamin Bohard

Message type

```
Tue 2022-10-25 09:38:57.016532 CEST [s=9d2d7a93fbd249f6bdd681abe25e9bdd;i=192e3;b=87547c6b9b4e49698e582470139257e8;m=126320c17d;t=5ebd7002d4d6e;x=e7d9d2e8b4699622]
    PRIORITY=6
    _SELINUX_CONTEXT=unconfined
    _SYSTEMD_SLICE=system.slice
    _BOOT_ID=87547c6b9b4e49698e582470139257e8
    _MACHINE_ID=2fba12537a944bfcb8dc4e5f1a933366
    _HOSTNAME=scribe
    _TRANSPORT=journal
    _UID=0
    _GID=0
    _CAP_EFFECTIVE=1fffffffff
    _SYSTEMD_CGROUP=/system.slice/eole-sso.service
    _SYSTEMD_UNIT=eole-sso.service
    CONTAINER_TAG=eole-sso
    CONTAINER_NAME=eolesso
    CODE_FILE=src/ctr_logging.c
    CODE_LINE=264
    CODE_FUNC=write_journald
    SYSLOG_IDENTIFIER=conmon
    _COMM=conmon
    _EXE=/usr/bin/conmon
```

```
    MESSAGE=comme sujet du certificat /etc/eolesso/eole.crt: 192.168.0.26
    _SYSTEMD_INVOCATION_ID=6a4cab08c250451382f7bffa51d9f76e
    CONTAINER_ID_FULL=c678e2b2475d601e45d52b68032217856d743437da8f6776e71e2612a9a49f44
    CONTAINER_ID=c678e2b2475d
    _PID=168074
    _CMDLINE=/usr/bin/conmon --api-version 1 -c c678e2b2475d601e45d52b68032217856d743437da8f6776e71e2612a9a49f
44 -u c678e2b2475d601e45d52b68032217856d743437da8f6776e71e2612a9a49f44 -r /usr/bin/crun -b /var/lib/containers
/storage/overlay-containers/c678e2b2475d601e45d52b68032217856d743437da8f6776e71e2612a9a49f44/userdata -p /run/
containers/storage/overlay-containers/c678e2b2475d601e45d52b68032217856d743437da8f6776e71e2612a9a49f44/userdat
a/pidfile -n eolesso --exit-dir /run/libpod/exits --full-attach -s -l journald --log-level warning --runtime-a
rg --log-format=json --runtime-arg --log --runtime-arg=/run/containers/storage/overlay-containers/c678e2b2475d
601e45d52b68032217856d743437da8f6776e71e2612a9a49f44/userdata/oci-log --log-tag eole-sso --conmon-pidfile /run
/containers/storage/overlay-containers/c678e2b2475d601e45d52b68032217856d743437da8f6776e71e2612a9a49f44/userda
ta/conmon.pid --exit-command /usr/bin/podman --exit-command-arg --root --exit-command-arg /var/lib/containers/
storage --exit-command-arg --runroot --exit-command-arg /run/containers/storage --exit-command-arg --log-level
 --exit-command-arg warning --exit-command-arg --cgroup-manager --exit-command-arg systemd --exit-command-arg
--tmpdir --exit-command-arg /run/libpod --exit-command-arg --runtime --exit-command-arg crun --exit-command-ar
g --events-backend --exit-command-arg journald --exit-command-arg container --exit-command-arg cleanup --exit-
command-arg --rm --exit-command-arg c678e2b2475d601e45d52b68032217856d743437da8f6776e71e2612a9a49f44
    _SOURCE_REALTIME_TIMESTAMP=1666683537016532


Tue 2022-10-25 09:38:57.016990 CEST [s=9d2d7a93fbd249f6bdd681abe25e9bdd;i=192d3;b=87547c6b9b4e49698e5824701392
57e8;m=126320bcad;t=5ebd7002d489e;x=f0b0ede69e1fb3dd]
    _TRANSPORT=stdout
    PRIORITY=6
    SYSLOG_FACILITY=3
    _SELINUX_CONTEXT=unconfined
    _SYSTEMD_SLICE=system.slice
    _BOOT_ID=87547c6b9b4e49698e582470139257e8
    _MACHINE_ID=2fba12537a944bfcb8dc4e5f1a933366
    _HOSTNAME=scribe
    _UID=0
    _GID=0
    _CAP_EFFECTIVE=1fffffffff
    SYSLOG_IDENTIFIER=podman
    _COMM=podman
    _EXE=/usr/bin/podman
    _SYSTEMD_CGROUP=/system.slice/eole-sso.service
    _SYSTEMD_UNIT=eole-sso.service
    MESSAGE=comme sujet du certificat /etc/eolesso/eole.crt: 192.168.0.26
    _PID=167948
    _CMDLINE=/usr/bin/podman run --log-driver=journald --log-opt tag=eole-sso -v /etc/ssl/certs:/etc/ssl/certs
:ro -v /etc/eolesso:/etc/eolesso -v /usr/share/sso/interface:/usr/share/sso/interface -v /usr/share/sso/app_fi
lters:/usr/share/sso/app_filters -p 8443:8443 --name eolesso --rm hub.eole.education/eole/eole-sso-server:dev
    _SYSTEMD_INVOCATION_ID=6a4cab08c250451382f7bffa51d9f76e
    _STREAM_ID=5dd7f5cf243341889cbe308525261c64
```

Et côté rsyslog, avec la transmission par journald sur la socket /dev/log :

```
Debug line with all properties:
FROMHOST: 'scribe.domscribe.ac-test.fr', fromhost-ip: '127.0.0.1', HOSTNAME: 'scribe.domscribe.ac-test.fr', PR
I: 14,
syslogtag 'conmon[165952]:', programname: 'conmon', APP-NAME: 'conmon', PROCID: '165952', MSGID: '-',
TIMESTAMP: 'Oct 25 09:28:08', STRUCTURED-DATA: '-',
msg: ' comme sujet du certificat /etc/eolesso/eole.crt: 192.168.0.26'
escaped msg: ' comme sujet du certificat /etc/eolesso/eole.crt: 192.168.0.26'
inputname: imuxsock rawmsg: '<14>Oct 25 09:28:08 conmon[165952]: comme sujet du certificat /etc/eolesso/eole.c
rt: 192.168.0.26'
$!:
$.:
$/:
```

On perd les champs en cours de route et comme la modification de APP-NAME avec le système de tag ne fonctionne pas, les options pour le filtrage s'amenuisent.

#4 - 25/10/2022 10:13 - Benjamin Bohard

Avec le conteneur mongodb, les journaux semblent associés à podman seulement, et pas à conmon. C'est peut-être parce que l'applicatif ne renvoie pas ses messages sur la sortie standard.
Un montage a été effectué pour récupérer les journaux de l'application dans /var/log/mongodb.

#5 - 25/10/2022 11:09 - Benjamin Bohard

Plusieurs solutions pour remettre les journaux dans le circuit rsyslog avec des filtres adéquats (par conteneur) :

- le tag (non fonctionnel sur ubuntu)
- l'écriture des journaux dans un fichier par conteneur et lecture de ces fichiers par rsyslog
- utilisation du module imjournal de rsyslog plutôt que imuxsock pour récupérer les métadonnées depuis les entrées de journald (lecture depuis le fichier de journald, performances dissuassives si utilisé sur l'ensemble des messages)

La première méthode serait la plus simple ~~mais ne semble pas envisageable~~ (voir patch joint depuis la note suivante).
La deuxième méthode nécessite de faire attention à la taille des fichiers de logs intermédiaires et ne permet pas forcément d'associer les logs du conteneurs avec les logs du service lui-même (une partie gérée par podman pour le lancement, l'arrêt, etc et une partie gérée également avec conmon).
La troisième méthode ne paraît pas raisonnable, l'écriture dans un fichier journald spécifique ne semblant pas possible.

```
/usr/bin/podman run --log-driver=k8s-file --log-opt path=/var/log/container-eolesso.log --log-opt max-size=10M
 -v /etc/ssl/certs:/etc/ssl/certs:ro -v /etc/eolesso:/etc/eolesso -v /usr/share/sso/interface:/usr/share/sso/i
nterface -v /usr/share/sso/app_filters:/usr/share/sso/app_filters -p 8443:8443  --name eolesso --rm hub.eole.e
ducation/eole/eole-sso-server:${CONTAINER_TAG}
```

```
module(load="imfile")
input(type="imfile" Facility="local0" File="/var/log/container-eolesso.log" Tag="eolesso")
```

Avec le problème de droits sur le fichier de log créé par podman (root:root vs syslog: nécessaire pour permettre à rsyslog de le lire).

#6 - 25/10/2022 14:41 - Benjamin Bohard

- Fichier 0002-Backport-logging.patch ajouté

Après test, il semble que le problème du tag provienne d'une mauvaise correspondance entre les versions de podman et de conmon distribuées par ubuntu.

Il manque, dans la version de conmon distribuée, la prise en compte de l'option. On peut patcher assez facilement pour que ce soit pris en compte.

#7 - 25/10/2022 16:09 - Benjamin Bohard

On peut forcer l'identifiant syslog dans le fichier .service avec le paramètre SyslogIdentifier. C'est à utiliser en conjonction avec les options StandardOutput et StandardError avec la valeur journal (valeur par défaut, https://www.freedesktop.org/software/systemd/man/systemd.exec.html).

Cette méthode convient pour les services (eole-sso, mongodb) mais n'est pas applicable pour l'application graphique era.
L'application era n'est pas lancé via un service (ce n'en est pas un) et un "transient service" avec systemd-run, qui permettrait de passer le paramètre SyslogIdentifier, ne permet pas d'accéder à l'affichage.
J'ai tendance à penser que ce n'est pas bloquant, les messages aboutissant sur la sortie standard, donc visibles dans le terminal depuis lequel la commande a été lancée. Ces messages sont également triés par rsyslog dans le dossier conmon pour les raisons décrites précédemment.

#8 - 26/10/2022 12:11 - Benjamin Bohard

- Statut changé de En cours à À valider

#9 - 26/10/2022 12:12 - Benjamin Bohard

- % réalisé changé de 0 à 100

#10 - 07/11/2022 13:27 - Ludwig Seys

- Statut changé de À valider à Résolu

#11 - 24/11/2022 15:03 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

Fichiers

0002-Backport-logging.patch	2,81 ko	25/10/2022	Benjamin Bohard