

Distribution EOLE - Demande #21656

DHCPD - 2.5.x - correction de droits sur un dossier / fichier

09/10/2017 12:53 - Richard Perruchet

Statut:	Classée sans suite	Début:	09/10/2017
Priorité:	Normal	Echéance:	
Assigné à:	Gérald Schwartzmann	% réalisé:	0%
Catégorie:		Temps estimé:	0.00 heure
Version cible:		Temps passé:	1.50 heure
Description			
<p>Bonjour,</p> <p>Je viens de remarquer que nous avons régulièrement des erreurs dans le syslog concernant le service dhcpd.</p> <p>Ces erreurs apparaissent apparemment seulement sur les versions 2.5.x :</p> <pre>2017-10-09T06:45:34.094944+02:00 scribe.lan dhcpd: Can't create new lease file: Permission denied 2017-10-09T07:46:42.633885+02:00 scribe.lan dhcpd: Can't create new lease file: Permission denied 2017-10-09T08:51:49.428561+02:00 scribe.lan dhcpd: Can't create new lease file: Permission denied</pre> <p>Par défaut, sur un 2.5, le propriétaire du dossier /var/lib/dhcp/ est "root" :</p> <pre>Fichier : «/var/lib/dhcp/» Taille : 4096 Blocs : 8 Blocs d'E/S : 4096 répertoire Périphérique : fc02h/64514d Inœud : 259293 Liens : 2 Accès : (0755/drwxr-xr-x) UID : (0/ root) GID : (0/ root) Accès : 2016-08-24 19:24:15.000000000 +0200 Modif. : 2017-10-07 02:11:27.947907944 +0200 Changt : 2017-10-07 02:11:27.947907944 +0200 Créé : -</pre> <p>Alors que sur un serveur en version 2.3, le propriétaire du dossier /var/lib/dhcp3/ est "dhcpd" :</p> <pre>File: «/var/lib/dhcp3/» Size: 4096 Blocks: 8 IO Block: 4096 répertoire Device: fc02h/64514d Inode: 129811 Links: 2 Access: (0755/drwxr-xr-x) Uid: (109/ dhcpd) Gid: (113/ dhcpd) Access: 2017-10-09 09:49:22.469315523 +0200 Modify: 2017-10-09 11:14:52.879298700 +0200 Change: 2017-10-09 11:14:52.879298700 +0200</pre> <p>J'avais changer les droits du dossier /var/lib/dhcp/ sur un 2.5 pour que le propriétaire soit dhcpd :</p> <pre>chown -R dhcpd:dhcpd /var/lib/dhcp</pre> <p>Mais après un upgrade, ces droits reviennent à root:root.</p> <p>Après vérifications, nous avons des erreurs sur seulement les versions 2.5.</p> <p>Je soupçonne le fait qu'il n'ai pas les bons droits pour créer un nouveau fichier "lease" dans le dossier; et que du coup il ne puisse attribuer une adresse ip valide au client.</p> <p>Est-il possible de corriger les droits par défauts pour le propriétaire dhcp ?</p>			

Historique

#1 - 10/10/2017 10:08 - Gérald Schwartzmann

Le problème est plus compliqué qu'il n'y paraît et traîne chez Ubuntu depuis 4 ans.

<https://bugs.launchpad.net/ubuntu/+source/isc-dhcp/+bug/1186662>

Les droits reviennent à root:root lorsqu'on relance le service.

D'après moi il n'y a pas de dysfonctionnement, seul la pollution des journaux est invalidante.

#2 - 10/10/2017 10:15 - Gérald Schwartzmann

Le contournement suivant fonctionne :

- Stop the DHCP server (service isc-dhcp-server stop)
- chown -R dhcpd:dhcpd /var/lib/dhcp
- Edit /etc/init/isc-dhcp-server.conf and remove (or comment out) the following section from near the end:

```
# The leases files need to be root:root even when dropping privileges
[ -e /var/lib/dhcp/dhcpd.leases ] || touch /var/lib/dhcp/dhcpd.leases
chown root:root /var/lib/dhcp /var/lib/dhcp/dhcpd.leases
if [ -e /var/lib/dhcp/dhcpd.leases~ ]; then
    chown root:root /var/lib/dhcp/dhcpd.leases~
fi
```

- Edit /etc/apparmor.d/local/usr.sbin.dhcpd and add:

```
# Allow lease file updates
capability dac_override,
```

- Reload AppArmor profiles (service apparmor reload)
- Restart DHCPd (service isc-dhcp-server start)

#3 - 11/10/2017 09:55 - Gérald Schwartzmann

- Assigné à mis à Gérald Schwartzmann

#4 - 14/11/2017 10:43 - Gérald Schwartzmann

Bonjour,

Avez-vous tester le contournement proposé ?

Cordialement

#5 - 24/11/2017 10:45 - Richard Perruchet

Gérald Schwartzmann a écrit :

Bonjour,

Avez-vous tester le contournement proposé ?

Cordialement

Bonjour,

Avec ce contournement, plus d'erreurs "Can't create new lease file: Permission denied", mais "Can't backup lease database /var/lib/dhcp/dhcpd.leases to /var/lib/dhcp/dhcpd.leases~: Operation not permitted".

Cordialement.

#6 - 02/02/2018 17:06 - Gilles Grandgérard

- *Statut changé de Nouveau à Classée sans suite*

Ok pour le contournement.

Domage pour les logs

On attend la clôture Ubuntu pour faire plus.