Guide pratique du logiciel Linux Crash

Adaptation française du *Linux Crash HOWTO*

Norman Patten `<nepatten CHEZ us POINT ibm POINT com>`

Adaptation française: Simon Depiets

Relecture de la version française: Karine Volpi

Préparation de la publication de la v.f.: Jean-Philippe Guérard

1.0.fr.1.0

2004-03-21

Historique des versions

Version 1.0.fr.1.0	2004-03-21	SD,KV,JPG
	Première adaptation française	
Version 1.0	2002-01-30	NM
	Version initiale — *Initial release.*	

Ce document décrit l'installation et l'utilisation du paquet LKCD (*Linux Kernel Crash Dump*). Ce paquet permet la récupération d'une copie de la mémoire suite à un plantage du noyau.

Table des matières

1. Introduction 1
- 1.1. Droits d'utilisation 2

2. Comment fonctionne LKCD 2
- 2.1. Ce dont vous aurez besoin 2

3. L'installation de LKCD 2
- 3.1. Installer depuis le code source 2
- 3.2. Compiler et installer les outils LKCD 3
- 3.3. Qu'est-ce qui est installé 3
- 3.4. Installer les outils LKCD à partir du paquet RPM 3
- 3.5. Appliquer le correctif au noyau 3
- 3.6. Compiler et installer le noyau 4

4. Installer, essayer et lancer crash 4
- 4.1. Installer crash dump 4
- 4.2. Essayer crash 4
- 4.3. Lancez crash 4

1. Introduction

Le projet *LKCD*[1] est un ensemble de correctifs du noyau Linux et d'outils permettant de sauvegarder une copie de la mémoire du noyau lorsque celui-ci panique. L'image mémoire du noyau permet une analyse après coup de la cause de sa panique. Ceci grâce aux outils inclus dans le paquet. La plupart des systèmes Unix commerciaux sont vendus avec des outils semblables. Sur Linux, cependant, ce paquet est assez nouveau et doit être ajouté manuellement. L'utilitaire LKCD n'est pas destiné à donner des informations utiles dans le cas d'une panique causée par un problème matériel ou lors d'une violation de la segmentation mémoire. Le paquet LKCD complet peut être téléchargé sur http://lkcd.sourceforge.net/.

[1] *Linux Kernel Crash Dump* — Sauvegarde de la mémoire du noyau Linux en cas de plantage.

1.1. Droits d'utilisation

Envoyez vos commentaires et corrections en anglais à `<nepatten CHEZ us POINT ibm POINT com>`.

Send feedback to `<nepatten AT us DOT ibm DOT com>`.

N'hésitez pas à faire parvenir tout commentaire relatif à la version française de ce document à `<commentaires CHEZ traduc POINT org>` en précisant le titre et la version de ce document.

2. Comment fonctionne LKCD

Quand un noyau rencontre certaines erreurs, il appelle la fonction `panic` qui est produite par une erreur irréversible. Lors d'une telle situation, LKCD réalisera une copie de la mémoire du noyau vers une zone pré-désignée. La zone est par défaut la partition d'échange principale (*primary swap*). Le noyau n'est pas complètement fonctionnel à cette étape, mais il y dispose de capacités suffisantes pour recopier la mémoire sur le disque. Lorsque la copie est terminée, le système redémarre.

Lors du redémarrage du système, si une nouvelle copie de la mémoire est trouvée sur la partition d'échange principale, elle est copiée par défaut vers le répertoire `/var/log/dump`. Une fois l'image recopiée, le démarrage se poursuit normalement et une analyse médico-légale pourra être effectuée plus tard.

2.1. Ce dont vous aurez besoin

Le fichier `lkcd-noyauxxx.diff` qui est un correctif à appliquer au noyau. La version du noyau à laquelle s'applique ce correctif change régulièrement.

`lkcdutils-xx.src.rpm` — ce sont les scripts et les sources des outils dont vous aurez besoin pour installer LKCD et lire la copie mémoire. Au moment où j'écris, il existe un paquet rpm binaire destiné aux processeurs i386. Il est disponible sur http://lkcd.sourceforge.net/. Cependant, vous aurez quand même besoin des correctifs à appliquer aux scripts de démarrage. Vous trouverez ces correctifs dans le paquet rpm des sources.

3. L'installation de LKCD

3.1. Installer depuis le code source

Téléchargez `lkcdutils-xxx.src.rpm` et installez le en utilisant la commande :

```
rpm -i kcdutils-xxx.src.rpm
```

Cela placera un fichier appelé `lkcdutils-xxx.tar.gz` dans le répertoire `/usr/src/redhat/SOURCES`. Ce fichier est une archive au format tar compressée de l'arborescence des sources de LKCD.

Décompressez les sources dans le répertoire de votre choix, comme par exemple `/usr/src` en utilisant la commande :

```
tar -zxvf kcdutils-xxx.src.rpm
```

Cela créera un répertoire appelé `kcdutils-xxx` contenant les sources des outils LKCD.

3.2. Compiler et installer les outils LKCD

LKCD utilise les fichiers make et le compilateur gcc standards. Pour compiler l'ensemble LKCD, rendez-vous au répertoire des sources de LKCD et lancez **`./configure`** pour fabriquer les fichiers de configuration. L'étape suivante est de lancer **`make`** pour compiler les outils et finalement **`make install`** pour installer les outils et les pages de manuels.

3.3. Qu'est-ce qui est installé

```
/etc/sysconfig/dump            # Configuration de dump (recopie mémoire)
/sbin/lcrash                   # L'outil « crash » (analyse
                               #  médico-légale)
/sbin/lkcd                     # Script de paramétrage du système
/sbin/lkcd_config              # Outil de configuration de « dump »
/sbin/lkcd_ksyms               # Outil de reconstruction des symboles du
                               #  noyau
/usr/include/sial_api.h        # Fichier d'en-têtes C des fonctions
                               #  utilisateurs SIAL
/usr/lib/libsial.a             # Bibliothèque SIAL (Langage Simple
                               #  d'Accès aux Images)
/usr/man/man1/lcrash.1         # Page de manuel de « lcrash »
/usr/man/man1/lkcd_config.1    # Page de manuel de « lkcd_config »
/usr/man/man1/lkcd_ksyms.1     # Page de manuel de « lkcd_ksyms »
/usr/share/sial/lcrash/ps.sial # Commande ps réalisée avec SIAL
```

3.4. Installer les outils LKCD à partir du paquet RPM

Vous pouvez installer les utilitaires pré-compilés à partir du paquet rpm en utilisant la commande :

```
rpm -i kcdutils-xxx.rpm
```

Vous aurez toujours à appliquer le correctif au noyau et à installer les scripts de démarrage. Cependant vous n'aurez pas à effectuer l'étape de compilation des outils.

3.5. Appliquer le correctif au noyau

L'étape suivante consiste à appliquer le correctif et à recompiler le noyau. Vous devrez appliquer au code source du noyau le correctif `lkcd-xxx.diff` que vous aurez téléchargé depuis http://lkcd.sourceforge.net/. Copiez le correctif dans le répertoire des sources noyau et lancez la commande :

```
patch -p0 < lkcd-noyauxxx.diff
```

Assurez-vous que le correctif que vous utilisez est bien pour votre version du noyau. Vous devrez ensuite configurer le noyau pour activer l'option « Kernel crash dumps ». Cette option est désactivée par défaut. Si vous utilisez **`make menuconfig`** ou **`make xconfig`**, vous trouverez cette option dans la section « Kernel hacking ». N'oubliez pas d'activer les fonctions du noyau dont votre système a besoin. Consultez le guide pratique du noyau Linux [http://www.traduc.org/docs/howto/lecture/Kernel-HOWTO.html] pour plus d'informations.

3.6. Compiler et installer le noyau

Il vous faut maintenant compiler et installer le noyau incluant le support LKCD. Dans le répertoire des sources du noyau, lancez dans l'ordre les commandes suivantes :

```
make depend
make install
make modules
make modules_install
```

Cela compilera et installera le nouveau noyau. Vous devrez aussi copier le fichier `Kerntypes` inclus dans les sources du noyau dans le répertoire `/boot`. Il sera peut-être également nécessaire d'éditer le fichier `lilo.conf` pour qu'il pointe vers votre nouveau noyau. Consultez le guide pratique du noyau Linux [http://www.traduc.org/docs/howto/lecture/Kernel-HOWTO.html] pour plus d'informations sur la compilation et l'installation d'un nouveau noyau.

4. Installer, essayer et lancer crash

4.1. Installer crash dump

Afin de pouvoir récupérer l'image mémoire qui a été écrite sur la partition d'échange, il est nécessaire de sauvegarder cette image mémoire avant que la partition d'échange n'aie été montée par le système. À cette fin, le fichier de démarrage sysinit doit être modifié. Le paquet des sources de LKCD inclut un répertoire `scripts` qui contient des correctifs pour plusieurs des scripts de démarrage sysinit. Ces correctifs ajoutent les commandes `lkcd config` et `lkcd save` pour activer la recopie mémoire en cas de panne et pour sauvegarder au démarrage une éventuelle copie mémoire préexistante.

4.2. Essayer crash

Pour forcer une panique afin d'essayer votre nouvelle installation de crash, compilez le code ci-dessous avec la commande : « **`cc -c -O2 -isystem /lib/modules/`uname -r`/build/include -Wall panic.c`** ». Après avoir compilé le module `panic.o`, il vous suffira d'utiliser la commande **insmod panic.o** pour déclencher une panique du noyau.

```
### panic.c ###########################
#define __KERNEL__
#define MODULE

#include <linux/module.h>

int init_module (void)
{
    panic(" panic a ete appele");
    return 0;
}
```

4.3. Lancez crash

Afin d'examiner votre sauvegarde de la mémoire du noyau, vous devrez lancer **lcrash** avec quelques paramètres :

```
lcrash [ fichier System.map ] [ copie de la mémoire ] [ Kerntypes ]
```

Par exemple :

```
lcrash /boot/System.map ./dump.1 /boot/Kerntypes
```

Le chargement de l'image mémoire prendra une minute avant que vous ne vous retrouviez dans l'interpréteur de commandes de crash. Vous pouvez taper un **?** pour obtenir la liste des commandes disponibles.