Gentoo

Desnos Anthony, Diascorn Ambroise

Ifsic - Université de Rennes 1

juin 2007

gentoo linux

Introduction

Historique

- Distribution dite *source*
- Crée par *Daniel Robbins* sous le nom de *Enoch Linux* en 1999
- *Gentoo Linux* 1.0 sortie le 31 mars 2002
- En 2004 la fondation Gentoo, association a but non-lucratif est crée
- Architectures supportées : x86, x86-64, IA-64, PA-RISC ; PowerPC 32/64, SPARC, DEC Alpha, ARM, MIPS, S390, sh, 68k
- Dernière version : 2007.0 / 7 Mai 2007

gentoo linux

Introduction

Philosophie

- LFS avec automatisation de la compilation
- Sélectionner les paquets
- Faciliter d'installation des paquets
- Compilation des paquets :
  - Choix des flags(ssl, X, etc)
  - Optimisation pour le processeur

gentoo linux

Introduction

Installation

- 2 types d'installation :
  - graphique
  - console

Introduction

Mode graphique

- Classique, comme les autres ditributions (click and install)
- Choix des paquets

gentoo linux

Introduction

Mode graphique

- Classique, comme les autres ditributions (click and install)
- Choix des paquets

Mode console

- Minimale :
  - Système de base (baselayout, coreutils, etc)
  - Système de paquets
  - Noyau
  - Aucun environnement graphique par défaut

gentoo linux

gentoo linux

Gestion des paquets

Portage

- Logiciel de gestion de paquets (BSD style)
- Complètement écrit en python et bash
- Utilisation principale à travers *emerge*

Gestion des paquets

Portage

- Logiciel de gestion de paquets (BSD style)
- Complètement écrit en python et bash
- Utilisation principale à travers *emerge*

Arbre de Portage

- Liste de répertoires(par défault /usr/portage/) contenant les *Ebuilds* :
  - Fichier qui contient toutes les informations que *Portage* a besoin pour l'installation du logiciel
  - Informations : version, dépendances, emplacement de téléchargement, etc...

Aperçu de portage

```
admin08 portage # ls -lh |cut -d " " -f1|cut -d "-" -f1 |grep d|wc -l
155
admin08 portage # ls
app-accessibility  app-office   dev-ml          games-engines  header.txt     net-dns       net-zope       skel.ChangeLog  www-client
app-admin          app-pda      dev-perl        games-fps      kde-base       net-firewall  perl-core      skel.ebuild     www-misc
app-antivirus      app-portage  dev-php         games-kids     kde-misc       net-fs        profiles       skel.metadata.xml  www-servers
app-arch           app-shells   dev-php4        games-misc     licenses       net-ftp       rox-base       sys-apps        x11-apps
app-backup         app-text     dev-php5        games-mud      mail-client    net-im        rox-extra      sys-auth        x11-base
app-benchmarks     app-vim      dev-python      games-puzzle   mail-filter    net-irc       sci-astronomy  sys-block       x11-drivers
app-cdr            app-xemacs   dev-ruby        games-roguelike  mail-mta     net-libs      sci-biology    sys-boot        x11-libs
app-crypt          dev-ada      dev-scheme      games-rpg      media-fonts    net-mail      sci-calculators  sys-cluster   x11-misc
app-dicts          dev-cpp      dev-tcltk       games-server   media-gfx      net-misc      sci-chemistry  sys-devel       x11-plugins
app-doc            dev-db       dev-tex         games-simulation  media-libs  net-nds       sci-electronics  sys-freebsd   x11-proto
app-editors        dev-dotnet   dev-tinyos      games-sports   media-plugins  net-news      sci-geosciences  sys-fs        x11-terms
app-emacs          dev-embedded  dev-util       games-strategy  media-radio   net-nntp      sci-libs       sys-kernel      x11-themes
app-emulation      dev-games    distfiles       games-util     media-sound    net-p2p       sci-mathematics  sys-libs      x11-wm
app-forensics      dev-haskell  eclass          gnome-base     media-tv       net-print     sci-misc       sys-power       xfce-base
app-i18n           dev-java     games-action    gnome-extra    media-video    net-proxy     sci-physics    sys-process     xfce-extra
app-laptop         dev-lang     games-arcade    gnustep-apps   metadata       net-voip      sci-visualization  virtual
app-misc           dev-libs     games-board     gnustep-base   net-analyzer   net-wireless  scripts        www-apache
app-mobilephone    dev-lisp     games-emulation  gnustep-libs  net-dialup     net-www       sec-policy     www-apps
admin08 portage #
```

gentoo linux

Make.conf

LE fichier de configuration

- Localisation : /etc/make.conf
- Composé de variables
- Partage des variables pour la compilation

Aperçu de make.conf

```
admin08 portage # cat /etc/make.conf
# These settings were set by the catalyst build script that automatically built this stage
# Please consult /etc/make.conf.example for a more detailed example
CFLAGS="-march=pentium4 -O2 -mtune=i686 -pipe"
CHOST="i686-pc-linux-gnu"
CXXFLAGS="${CFLAGS}"

INPUT_DEVICES="keyboard mouse"
VIDEO_CARDS="vesa vga fbdev i810"
GENTOO_MIRRORS="http://ftp.belnet.be/mirror/rsync.gentoo.org/gentoo/ ftp://ftp.belnet.be/mirror/rsync.gentoo.org/gentoo/ "
LINGUAS="fr"
ALSA_CARDS="intel8x0"

USE="X gtk gnome hal ssl cups ldap alsa gstreamer nptl nptlonly motif latex tk -qt3 -qt4 -arts -kde -ipv6"
admin08 portage #
```

Make.conf

USE

- Spécifier les options par défaut
- Activé seulement par les paquets supportant l'option
- Plus de 60 options de compilation
- Exemples : alsa, emacs, ssl, ldap, png, mp3 ...

Make.conf

CFLAGS

- Système de paquetage classique : i386 pour assurer la compatibilitée pour tous les processeurs
- Compiler les programmes spécifiquement pour le processeur (Intel (pentium (I, PRO, II, III, 4, D), Xeon, core), VIA, TRANSMETA, AMD, POWERPC, SPARC, etc)
- Optimiser les performances des programmes
- Exemples : -march=pentium4 -O2 -mtune=i686 -pipe

gentoo linux

Make.conf

CHOST

- Indiquer l'architecture de la machine
- Exemples : pentium4 i686

Emerge

Interface en ligne de commande pour utiliser *Portage*

- Utilise par défaut Make.conf
- Mise à jour (emerge –sync)
- Installation de paquet (emerge paquet)
- Désinstallation de paquet (emerge -C paquet)
- Gestion des dépendances

gentoo linux

Gentoolkit

Collection d'outils pour l'administration

- Equery : afficher toutes les informations sur les paquets ou fichiers
- Euse : manipler les flags

Equery

```
proj20 ~ # equery belongs /etc/conf.d/local.start
[ Searching for file(s) /etc/conf.d/local.start in *... ]
sys-apps/baselayout-1.12.9-r2 (/etc/conf.d/local.start)
proj20 ~ # equery belongs /bin/cat
[ Searching for file(s) /bin/cat in *... ]
sys-apps/coreutils-6.7-r1 (/bin/cat)
proj20 ~ # equery check vim
[ Checking app-editors/vim-7.0.174 ]
 * 6 out of 6 files good
proj20 ~ # equery depends subversion
[ Searching for packages depending on subversion... ]
dev-perl/SVN-Mirror-0.73 (>=dev-util/subversion-1.1.3)
dev-perl/SVN-Simple-0.27 (>=dev-util/subversion-0.31)
dev-util/svk-1.08 (>=dev-util/subversion-1.0.7)
proj20 ~ # equery files vim
[ Searching for packages matching vim... ]
* Contents of app-editors/vim-7.0.174:
/usr
/usr/bin
/usr/bin/rview -> vim
/usr/bin/rvim -> vim
/usr/bin/vim
/usr/bin/vimdiff -> vim
proj20 ~ # equery hasuse png
[ Searching for USE flag png in all categories among: ]
 * installed packages
[I--] [  ] app-editors/xemacs-21.4.20-r1 (0)
[I--] [  ] media-gfx/gimp-2.2.14 (2)
[I--] [  ] media-gfx/imagemagick-6.3.3 (0)
[I--] [  ] media-gfx/xloadimage-4.1-r4 (0)
[I--] [  ] media-gfx/splashutils-1.4.2 (0)
[I--] [  ] sci-visualization/gnuplot-4.0-r1 (0)
[I--] [  ] dev-scheme/drscheme-360-r1 (0)
[I--] [  ] media-libs/netpbm-10.37.0 (0)
[I--] [  ] media-libs/imlib2-1.3.0 (0)
[I--] [  ] media-libs/gd-2.0.34 (2)
[I--] [  ] x11-libs/qt-4.2.3-r1 (4)
[I--] [  ] media-video/vlc-0.8.6-r1 (0)
[I--] [  ] net-print/cups-1.2.9 (0)
proj20 ~ #
```

gentoo linux

Equery

```
clio ~ # equery uses emacs
[ Searching for packages matching emacs... ]
[ Colour Code : set unset ]
[ Legend : Left column  (U) - USE flags from make.conf                ]
[        : Right column (I) - USE flags packages was installed with ]
[ Found these USE variables for app-editors/emacs-21.4-r12 ]
 U I
 + + X           : Adds support for X11
 + + Xaw3d       : Adds support of the 3d athena widget set
 - - leim        : Adds input methods support to Emacs
 + + lesstif     : Use lesstif over openmotif in cases where a program supports both
 - - motif       : Adds motif support (x11-libs/openmotif x11-libs/lesstif)
 + + nls         : Adds Native Language Support (using gettext - GNU locale utilities)
 - - nosendmail  : If you do not want to install any MTA
clio ~ # equery size vlc
[ Searching for packages matching vlc... ]
* size of media-video/vlc-0.8.6-r1
            Total files : 539
     Inaccessible files : 3
            Total size  : 6043.40 KiB
clio ~ #
```

gentoo linux

Mise à jour

Profile

- Suivre l'évolution de gentoo(avoir toujours une distribution à jour)
- Migrer vers un profil différent facilement

Mise à jour

Profile

- Suivre l'évolution de gentoo(avoir toujours une distribution à jour)
- Migrer vers un profil différent facilement

Liste des profils

```
admin08 portage # eselect profile list
Available profile symlink targets:
  [1]   default-linux/x86/2006.1
  [2]   default-linux/x86/no-nptl
  [3]   default-linux/x86/no-nptl/2.4
  [4]   default-linux/x86/2006.1/desktop
  [5]   default-linux/x86/2007.0
  [6]   default-linux/x86/2007.0/desktop *
  [7]   hardened/x86/2.6
  [8]   selinux/x86/2006.1
```

Mise à jour

Selection du profil

- Migrer vers un profil sécurisé ?
- eselect profile set 7

Mise à jour

Synchronisation de *Portage*

- emerge –sync
- emerge-webrsync (pour le filtrage)

Mise à jour

Paquet particulier

- emerge paquet

Mise à jour

Paquet particulier

- emerge paquet

Paquets installés

- Catégorie *World* : installé après le système de base
- emerge -uDv world

gentoo linux

Mise à jour

Système

- Catégorie *System* : système de base
- emerge -uDv system

Mise à jour

Système

- Catégorie *System* : système de base
- emerge -uDv system

Compilateur

- Recompilation de **TOUT** le système
- Lancer le vendredi soir, fini le lundi matin

gentoo linux

Mise à jour

Sécurité

- Réactivitée très rapide pour les failles de sécurité
- GLSA

gentoo linux

Mise à jour

Sécurité

- Réactivitée très rapide pour les failles de sécurité
- GLSA

GLSA : Gentoo Linux Security Advisories

- url : http ://www.gentoo.org/security/en/glsa/

GLSA Advisory

ClamAV: Multiple Denials of Service

Content: 1. Gentoo Linux Security Advisory

1. Gentoo Linux Security Advisory

Version Information

Advisory Reference	GLSA 200706-05 / clamav
Release Date	June 15, 2007
Latest Revision	June 15, 2007: 01
Impact	normal
Exploitable	remote, local

Package	Vulnerable versions	Unaffected versions	Architecture(s)
app-antivirus/clamav	< 0.90.3	>= 0.90.3	All supported architectures

Related bugreports: #178082

Synopsis

ClamAV contains several vulnerabilities leading to a Denial of Service.

GLSA Impact Information

2. Impact Information

Background

ClamAV is a GPL virus scanner.

Description

Several vulnerabilities were discovered in ClamAV by various researchers:

- Victor Stinner (INL) discovered that the OLE2 parser may enter in an infinite loop (CVE-2007-2650).
- A boundary error was also reported by an anonymous researcher in the file unsp.c, which might lead to a buffer overflow (CVE-2007-3023).
- The file unrar.c contains a heap-based buffer overflow via a modified vm_codesize value from a RAR file (CVE-2007-3123).
- The RAR parsing engine can be bypassed via a RAR file with a header flag value of 10 (CVE-2007-3122).
- The cli_gentempstream() function from clamdscan creates temporary files with insecure permissions (CVE-2007-3024).

Impact

A remote attacker could send a specially crafted file to the scanner, possibly triggering one of the vulnerabilities. The two buffer overflows are reported to only cause Denial of Service. This would lead to a Denial of Service by CPU consumption or a crash of the scanner. The insecure temporary file creation vulnerability could be used by a local user to access sensitive data.

GLSA Resolution Information

3. Resolution Information

Workaround

There is no known workaround at this time.

Resolution

All ClamAV users should upgrade to the latest version:

Code Listing 3.1

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=app-antivirus/clamav-0.90.3"
```

gentoo linux

GLSA

glsa-check

- Outil permettant de gérer localement les GLSA
  - Visualiser les publications de failles
  - Appliquer les correctifs automatiquement

glsa-check

```
clio ~ # glsa-check -p $(glsa-check -t all)
This system is affected by the following GLSAs:
Checking GLSA 200705-24
The following updates will be performed for this GLSA:
     media-libs/libpng-1.2.18 (1.2.16)

Checking GLSA 200705-25
The following updates will be performed for this GLSA:
     sys-apps/file-4.21 (4.20-r1)

Checking GLSA 200706-01
The following updates will be performed for this GLSA:
     media-libs/libexif-0.6.15 (0.6.13-r1)

clio ~ #
```

gentoo linux

Divers

Epurer les paquets

- Dépendances inutiles suites à des mises à jour
- emerge -v depclean

gentoo linux

Divers

Epurer les paquets

- Dépendances inutiles suites à des mises à jour
- emerge -v depclean

Vérifier les librairies partagées

- Réparer les binaires ou librairies à qui il manque des bibliothèques partagées
- Reverse Dependency Rebuilder : revdep-rebuild -v

gentoo linux

Divers

Sécuriser grub

- Non sécurisé par défaut
- Accès au système de fichier sans authentification

gentoo linux

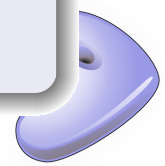
Divers

Sécuriser grub

- Non sécurisé par défaut
- Accès au système de fichier sans authentification

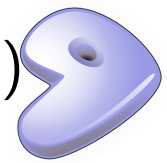
Résolution

- Demande de mot de passe pour effectuer une maintenance
- grub-md5-crypt : récupére un mot de passe chiffré
- password –md5 **PASSWORDCHIFFRE** : ajouter dans grub.conf



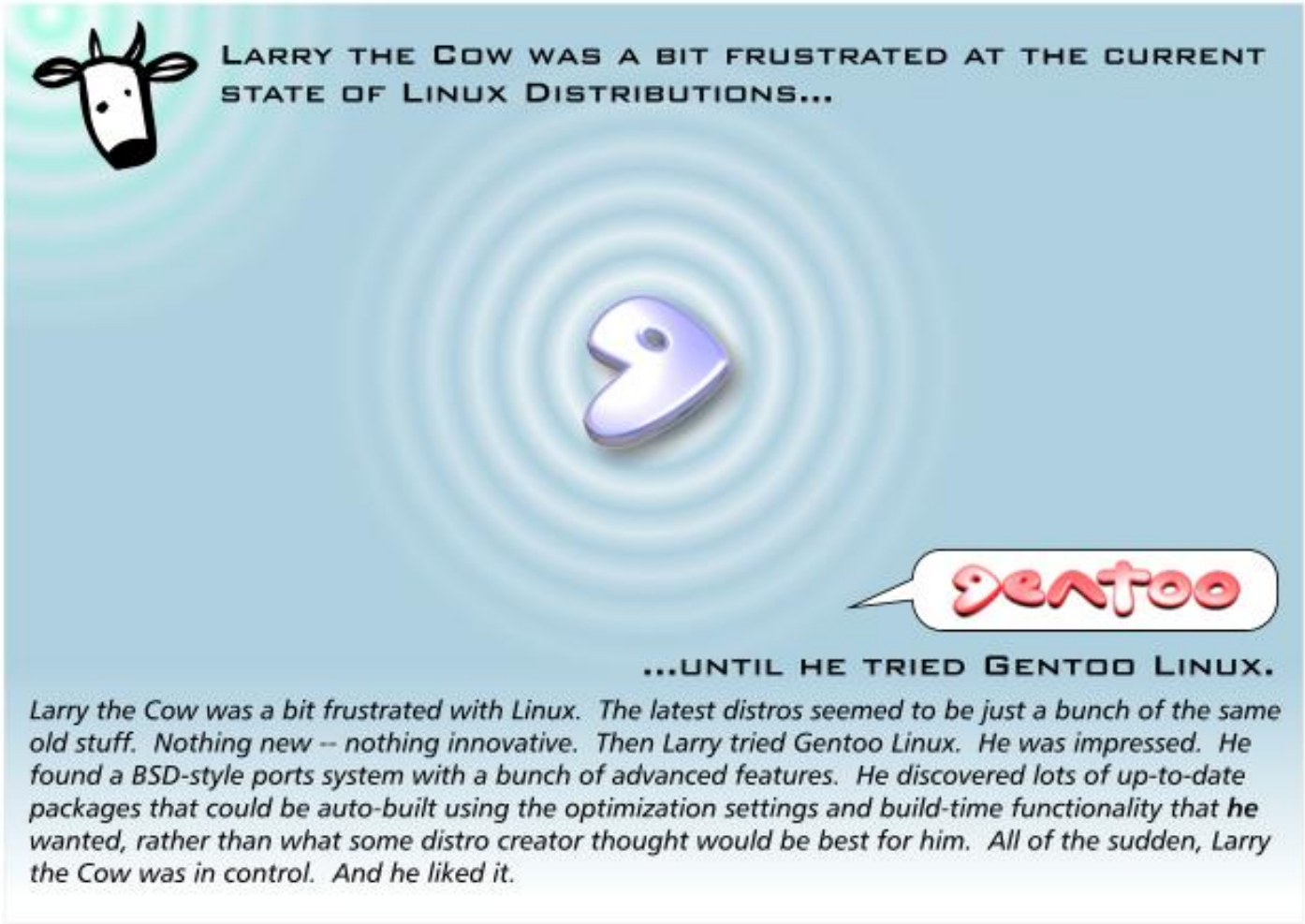
Conclusion

- Installation **beaucoup** plus longue que les autres distributions (temps perdu)
- Faciliter de maintenance (temps gagné)
- Evolution constante
- Paquets toujours à jour
- Choix des paquets impressionant avec différentes versions
- Mise à jour de sécurité
- Optimisation des performances par la compilation spécifique
- Grande communautée très réactif (forum, wiki, bugtrack, etc)



gentoo linux

Questions ?



gentoo linux