



88 rue d'Eaubonne  
95100 ARGENTEUIL  
Tél : +33.(0)1.34.11.20.97  
Fax : +33.(0)1.34.10.13.74  
contact@derternet.com  
<http://www.derternet.com>

## **NOTIONS DE SECURITE INFORMATIQUE** **SERVEURS SOUS LINUX**

Version 1.4 (20 mars 2006)

### **1) Linux**

#### **1) Qu'est-ce que Linux ?**

Linux est un système d'exploitation. Un système d'exploitation est un ensemble d'instructions informatiques qui pilotent une machine (par exemple un serveur) pour réaliser des tâches particulières.

Linux est le système d'exploitation utilisé en standard sur tous les serveurs dédiés DERTERNET et est également le système d'exploitation utilisé en standard par DERTERNET dans le cadre de ses prestations d'hébergement web mutualisé, semi-dédié et dédié.

Ce système d'exploitation est développé et maintenu par une équipe internationale de programmeurs bénévoles.

#### **2) Unix et création de Linux**

Unix est le système d'exploitation qui a servi de modèle à Linux. Unix est un système d'exploitation multitâche et multiutilisateurs qui a été développé en 1969 par Ken Thompson.

Ré-écrit en C par Ken Thompson en 1973, Unix a été porté sur de nombreuses machines et fut à l'époque le système d'exploitation le plus répandu.

Le créateur de Linux est un étudiant Finlandais appelé Linus Torvald. Linux a été développé en 1991 (la version 0.01 fut diffusée en août 1991). La version 1.0 apparut en mars 1994.

#### **3) Les distributions**

Linux est simplement le noyau du système d'exploitation. Une distribution Linux est donc le noyau (kernel) + d'autres logiciels libres qui sont apparus au fil des années (les utilitaires GNU).

Etant donné la complexité et la souplesse du système d'exploitation, Linux peut revêtir plusieurs formes. Les distributions majeures de Linux sont (dans l'ordre alphabétique) :

- Debian
- Mandrake
- OpenLinux (Caldera)
- RedHat
- Slackware
- SuSE

Il existe environ 200 distributions Linux différentes.

DERTERNET utilise en standard la distribution SuSE qui est originaire d'Allemagne, qui a une excellente finition, une très bonne qualité et est utilisée également en standard chez ses fournisseurs allemands.

Voici 2 liens vers les distributions Linux :

<http://www.linux.org/dist/index.html>

<http://linux-france.org/article/choix-distri/>

## **II) Maintenance, administration et sécurité du système**

### **1) Maintenance et gestion du système de fichier**

Quelle que soit la distribution Linux que vous avez chez DERTERNET, vous devez veiller au bon fonctionnement de votre système de fichiers pour que votre serveur fonctionne correctement.

Si vous arrêtez votre serveur avec la commande shutdown, utilisez l'option -f pour omettre la vérification du système de fichiers lorsqu'il redémarrera. Linux vous laissera utiliser cette option à plusieurs reprises mais il décidera du moment où il faudra impérativement procéder à une vérification. Bien que l'option -f permette de gagner du temps, il ne faut pas en abuser. La vérification du système de fichiers nécessite 1 minute de plus au démarrage mais elle vous épargnera les problèmes au cas où vous auriez à réparer une défaillance. Vous pouvez vérifier manuellement les systèmes de fichiers en utilisant la commande e2fsck.

Pour rebooter votre serveur, utilisez de préférence la commande « shutdown -r now »

### **2) Répartition des zones à problèmes**

Certaines personnes procèdent souvent à plusieurs réinstallations de programmes avant d'être vraiment satisfaites. Pour cette raison, vous pouvez placer les parties de votre système de fichiers sujettes à de fréquents changements sur une partition qui leur soit propre. Traditionnellement, ces segments sont les répertoires /var et /tmp. Ces parties du système de fichiers peuvent changer plusieurs fois. Si les modifications sont trop répétitives, cela peut conduire à une dégradation du disque.

### **3) Espace disque**

L'insuffisance de l'espace disque est un des problèmes insidieux du système d'exploitation. Si votre partition racine est remplie à 99 ou 100%, vous devrez utiliser les disquettes de secours pour faire démarrer la machine et la nettoyer.

En général, aucune précaution n'est prise pour stocker des informations sur les disques, sauf si vous avez été sensibilisé par un manque de place lors de la mise en place de votre serveur. Plus vous travaillez, plus vous vous relâchez et plus vous oubliez de vérifier l'espace disque disponible. Ce problème arrive même aux administrateurs expérimentés. Pour l'éviter, faites des vérifications régulières sur l'occupation de vos disques.

### **4) La sécurité**

Lorsque vous partez de chez vous, laissez-vous la porte ouverte ?

De nombreuses personnes font la même chose avec leur serveur et n'en ont même pas conscience !

La première protection est l'ensemble des mots de passe du système. Si un compte possède un mot de passe simple à deviner, attendez-vous à des problèmes. N'utilisez par exemple jamais une partie de votre nom, du nom de vos amis, famille, animaux domestiques, dates de naissance...

Utilisez une combinaison de lettres minuscules/majuscules, chiffres et signes de ponctuation. Le mot de passe doit contenir au moins 8 caractères.

Par défaut, DERTERNET et Confixx vous fournissent ce type de mot de passe. Bien sûr, ne fournissez votre mot de passe qu'à des personnes sérieuses et expérimentées.

Mettez également à jour régulièrement les logiciels présents sur votre serveur (ProFTPD, Apache, Postfix, PHP, ...).

L'administrateur d'un système Linux doit être vigilant. En tant que responsable, vous devez vous assurer que votre serveur n'accueille pas d'intrus.

*Vous devez donc obligatoirement mettre à jour les corrections de sécurités. Tout système d'exploitation a des trous de sécurité, ils sont inévitables !*

Pensez également à ne pas démarrer les services réseau dont vous n'avez pas besoin. Ce sont autant de portes d'entrée sur votre serveur !

Si quelqu'un entre sur votre serveur, vous aurez des soucis supplémentaires liés à la sécurité. Cette personne peut endommager votre système en exécutant un ou plusieurs programmes dont les permissions n'étaient pas assez restrictives. Dans ce cas, ce sera la catastrophe pour vous.

*Votre serveur étant connecté à Internet 24h/24 et 7j/7, n'oubliez jamais de sécuriser votre système !*

### **5) Le kernel**

Le kernel (noyau) est le cœur de Linux. Quelque soit la tâche que votre serveur exécute, celle-ci passe par le noyau. C'est donc l'élément à mettre à jour en priorité. Cette tâche reste toutefois assez fastidieuse pour les personnes qui ne connaissent pas trop Linux.

A titre informatif, il existe un bug dans le noyau Linux qui permet à une personne distante de devenir superadministrateur (root) sur votre serveur.

TOUS LES NOYAUX LINUX SONT CONCERNES SAUF :

2.2.26

2.4.26

2.6.5

2.6.6

2.6.7 et supérieurs

DERTERNET conseille donc vivement à tous ses clients de mettre à jour leurs noyaux Linux.

Cette opération étant une opération lourde (qui demande un redémarrage complet du serveur), DERTERNET peut faire cette opération sur simple demande dans le cadre d'une prestation d'ingénierie serveur (50 euros HT).

## **III) DERTERNET, politique de sécurité et informations diverses**

### **1) DERTERNET**

Dans le cadre des prestations d'hébergements mutualisés, le client n'a pas à se soucier de la sécurité, de l'administration, des mises à jours et de la surveillance du serveur sur lequel son compte web est installé. Il est toutefois recommandé de faire des chmod appropriés sur les répertoires sensibles.

Dans le cadre des serveurs semi-dédiés WebOne et Web+, le client n'a pas à se soucier de la sécurité, de l'administration, des mises à jours et de la surveillance du serveur sur lequel son compte web est installé. Il est toutefois recommandé de faire des chmod appropriés sur les répertoires sensibles.

Dans le cadre des serveurs virtuels Root et WebRoot, la sécurité, l'administration, les mises à jour et la surveillance logicielle du serveur virtuel sont de la responsabilité du client. DERTERNET s'occupera uniquement de la mise à jour du kernel.

Dans le cadre des serveurs dédiés, la sécurité, l'administration, les mises à jour et la surveillance logicielle du serveur sont de la responsabilité du client.

A noter que DERTERNET propose des services afin que vous n'ayez pas à vous soucier de tout ça si vous le souhaitez. Ces services sont disponibles sur la page <http://www.derternet.com/ingenierieserveur.php>

## **2) Politique de sécurité**

Dans le cadre des prestations d'hébergements mutualisés ainsi que sur les points développés à propos des serveurs semi-dédiés WebOne et Web+, DERTERNET s'engage à faire le nécessaire sur les serveurs concernés.

Pour les serveurs virtuels Root/WebRoot et les serveurs dédiés sous Linux, DERTERNET fournit régulièrement via des alertes mails ainsi que dans sa newsletter mensuelle des informations sur les dernières failles de sécurité découvertes ainsi que des conseils pour les boucher et/ou mieux administrer votre serveur.

DERTERNET encourage vivement ses clients à avoir une politique d'administration et de sécurité système. En cas de piratage et/ou de crash de la machine en raison d'une faille de sécurité ou d'un bug non résolu, le client est responsable des éventuelles conséquences.

Un piratage (suivant ce qui a été fait sur le serveur) peut entraîner la perte totale des données et/ou un travail fastidieux pour remonter le système. Tous les frais liés à ce type d'opération sont de la responsabilité du client. C'est pourquoi DERTERNET préfère prévenir que guérir (même si on peut toujours remonter un système).

Nos services d'ingénierie serveur peuvent bien sûr résoudre tous ces soucis facilement

<http://www.derternet.com/ingenierieserveur.php>

## **3) Informations diverses**

Dans le cadre des serveurs virtuels Root et WebRoot, le client a accès à tous les programmes de son serveur (puisque'il a un accès SSH). Le seul élément auquel le client n'a pas accès est le kernel (celui-ci étant géré au niveau du serveur maître) et Iptables. DERTERNET s'occupera donc des mises à jour du kernel.

Dans le cadre des serveurs dédiés, le client a accès à 100% de son serveur et peut faire ce qu'il veut dessus. Attention, en cas de crash système provoqué par une erreur du client et si DERTERNET doit intervenir pour relancer le système, l'opération sera prise en compte selon les conditions contractuelles.

## **IV) Mon serveur ne fonctionne plus. Que faire ?**

### **1) Rappels des règles contractuelles**

Linux, l'interface d'administration (et le serveur en général) sont installés avec une configuration par défaut. Le serveur est livré au client en état de marche avec cette configuration.

Le client est informé que Confixx est un outil d'appoint lui permettant de simplifier les tâches courantes (création de comptes web, de comptes POP, de bases de données, ...) via une interface web et que Confixx gère certains paramètres de manière personnelle qui peuvent nécessiter une réadaptation en cas de besoins spécifiques du client (scripts, applications ou configuration web non-standard). Le client reconnaît par la signature du contrat que cette configuration lui convient au moment de l'installation du serveur. Libre à lui ensuite de modifier cette configuration sous sa responsabilité.

Un support technique de premier niveau est assuré gratuitement tous les jours par email/fax/téléphone. Cela inclus toutes les demandes techniques standards.

*Le client s'engage à utiliser le téléphone uniquement pour les urgences.*

Aucune question rentrant dans le cadre du support technique de second niveau ne peut être demandé à DERTERNET via le support de premier niveau (sauf si le client passe une commande de support

de second niveau ou a l'option Gold). Cela inclut la programmation HTML, PHP, MySQL, Perl, ..., les chmods, les mises à jour de programmes, la configuration de programmes, l'installation de tâches cron, les redémarrages de services, la surveillance logicielle du serveur, les upgrades hardwares, la mise en place d'une politique de sécurité, la maintenance du système et plus généralement toute tâche nécessitant un accès via SSH et/ou interface autre que Confixx au serveur.

## **2) Support technique de troisième niveau chez DERTERNET**

Un support technique de troisième niveau (également appelé ingénierie serveur, administration système, sysadmin work ou administration Linux) peut être demandé à DERTERNET selon les conditions prévues dans les « Autres Conditions Contractuelles » du contrat signé.

DERTERNET se réserve le droit de refuser un support technique de troisième niveau si l'objet ne fait pas partie de ses compétences internes. Le support de second ou troisième niveau est assuré selon les disponibilités de DERTERNET.

Tarif général : 25 euros par quarts d'heure nécessaires à la tâche

## **3) Procédure de rétablissement**

Si votre serveur dédié ne fonctionne plus, tout d'abord dites-vous que sous Linux il y a toujours une solution.

Deuxièmement, vérifiez dans le monitoring d'Inetbone (<https://monitoring.inetbone.net>) si c'est seulement 1 service ou l'ensemble du serveur qui ne répond plus.

Si c'est juste un service, connectez-vous par SSH et redémarrez le service.

*Linux n'a pas besoin d'un reboot pour un simple problème de service crashé.*

Si c'est l'ensemble du serveur, essayez de vous connecter par SSH et tapez « shutdown -r now ». Si le SSH ne répond plus, alors seul un accès local pourra redémarrer la machine (dans ce cas, contactez DERTERNET dès que possible pour demander un reboot local).

## **4) Cause d'un crash**

Tout d'abord, il faut bien séparer les crashes services (par exemple juste Apache qui ne fonctionne plus) et les crashes système (plus rien ne fonctionne).

- La cause principale d'un crash service est la sur-utilisation du service. Par exemple, votre serveur reçoit trop de requêtes HTTP et donc le service va être surchargé et donc crasher. Ou bien (généralement pour Apache, même si ça reste un événement rare) par simple « usure ».

Pour prévenir ce risque, il existe 3 solutions :

- a) Installer une tâche cron de redémarrage du service (attention, en cas de crash système la tâche cron ne pourra pas s'exécuter, ainsi qu'en cas de manque de mémoire)
- b) Augmenter la RAM du serveur (pour pouvoir gérer davantage de processus)
- c) Mettre à jour le programme lançant le service lorsque des patches sortent.

- La cause principale d'un crash système est souvent le manque de mémoire ou l'utilisation incorrecte d'une commande.

Pour prévenir ce risque, il existe 4 solutions :

- a) Vérifier, avant de taper la commande, que vous tapez bien la bonne commande
- b) Augmenter la RAM du serveur
- c) Surveiller l'activité du serveur
- d) Mettre à jour régulièrement son serveur

Un crash service ou système peut également être provoqué par un problème hardware, un piratage, une attaque DOS ou l'exploitation d'un trou de sécurité.

Ces possibilités de crash peuvent être contrées simplement par l'utilisation de hardware de qualité, par la surveillance du serveur, la mise en place d'une politique de sécurité et la mise à jour régulière du serveur.

DERTERNET fournit bien sûr plusieurs services pour limiter les probabilités de crash.

Le client est toutefois informé qu'on ne peut que réduire les probabilités. Même si aujourd'hui, en faisant tout correctement, on approche véritablement des 100% de fiabilité, l'informatique peut réserver parfois quelques surprises et personne ne peut assurer un 100% pur sur de longues périodes.

### **5) Les 3 règles à ne jamais oublier**

- a) Mettre à jour son serveur dès qu'une faille de sécurité est découverte
- b) Prévoir une procédure en cas de crash système complet (serveur de secours, disque dur d'avance, backup automatique, ...)
- c) Sauvegarder très régulièrement les données présentes sur le serveur

### **6) J'ai été piraté. Que faire ?**

Tout d'abord, il faut distinguer 2 types de piratage :

- La simple intrusion
- La volonté de nuire

#### **La simple intrusion**

Symptômes : votre serveur ne fonctionne plus comme habituellement (par exemple certaines commandes ne fonctionnent plus correctement, de nombreux mails sont envoyés, une tâche prend toutes les ressources, ...)

Solution : Réinstaller les commandes/packages modifiés, vérifier les programmes lancés, mettre à jour le serveur

#### **La volonté de nuire**

Symptôme : Plus d'accès au serveur et/ou impossibilité de le redémarrer (même en accès local)

Solution : Essayer de le redémarrer en local. Si ça ne fonctionne pas, alors il faut réinstaller le système.

### **7) Procédures clients et DERTERNET**

Rappel : En cas de piratage, le client est responsable (sauf accords contraires indiqués dans le contrat).

Il est sensé avoir prévu une procédure au cas où cela arriverait.

Dans le cas où le client n'a rien prévu, il bénéficie de la procédure DERTERNET (149 euros HT). Cette procédure consiste à remonter le système en local dans les plus brefs délais. Lors de cette procédure, le système est remonté comme à son origine (les données perdues restent perdues).

Enfin, il peut utiliser la procédure DERTERNET avec rétablissement des données (249 euros HT) ; Cette procédure consiste à remonter le système en local dans les plus brefs délais et à récupérer les données (si elles sont récupérables, mais DERTERNET fera tout pour).

## **V) Sécurité informatique**

### **1) Principes généraux**

La sécurité informatique consiste à se protéger et à détecter une utilisation non-autorisée du serveur. Les mesures de prévention vous aident à arrêter les utilisateurs non-autorisés qui se connectent sur votre serveur.

Aujourd'hui, nous utilisons des serveurs Internet pour beaucoup de choses. Vous ne voulez sûrement pas que des intrus lisent vos mails, utilisent votre serveur pour attaquer d'autres systèmes ou consultent les fichiers présents.

Les pirates informatiques ne tiennent pas compte de votre identité. Souvent ils veulent juste obtenir le contrôle du serveur afin d'en attaquer d'autres. En ayant le contrôle de votre serveur, ils peuvent

cacheur leur identité et lancer des attaques. Même un serveur tout simple peut être la cible d'un pirate informatique. Un intrus peut voir toutes vos actions sur le serveur ou causer des dommages en reformatant le disque dur ou en modifiant des données.

Les pirates informatiques cherchent toujours les nouvelles vulnérabilités d'un système pour pouvoir y accéder. Quand une vulnérabilité est découverte, les éditeurs des programmes sortent généralement un patch pour corriger le problème. Cependant, c'est à vous de télécharger le patch et de l'installer. La plupart des problèmes peuvent être évités simplement en mettant à jour votre système.

## **2) Adresses IP**

Une adresse IP est comme un numéro de téléphone. Quand vous téléphonez à quelqu'un, vous devez au préalable connaître son numéro de téléphone. De manière similaire, quand un serveur sur l'Internet doit envoyer des données à une autre machine connectée, il doit d'abord connaître son adresse IP. Les adresses IP sont généralement représentées par 4 nombres séparés par des points. Par exemple 10.24.254.3 et 192.168.62.231 sont des adresses IP.

Si vous avez besoin de téléphoner à quelqu'un mais que vous ne connaissez que son nom, vous pouvez trouver son numéro dans l'annuaire. Sur Internet, cet annuaire est appelé Domain Name System (DNS). Si vous connaissez le nom d'un serveur et que vous le tapez dans un navigateur web, votre ordinateur demandera alors à son serveur DNS quelle adresse IP est associée à ce nom. Chaque serveur/ordinateur connecté à Internet a une adresse IP qui le définit de manière unique.

## **3) Risques**

La sécurité informatique est définie par 3 points :

- La confidentialité : les informations doivent être disponibles uniquement à ceux qui en ont les droits
- L'intégrité : les informations doivent être modifiables uniquement par ceux qui sont autorisés à le faire
- La disponibilité : les informations doivent être accessibles par ceux qui en ont besoin lorsqu'ils en ont besoin

Ces principes sont applicables à tous. Voici les méthodes les plus utilisées pour obtenir le contrôle d'une machine connectée à Internet.

- Trojans
- Backdoors
- Déni de Service
- Etre un intermédiaire pour une autre attaque
- Répertoires non protégés
- Code mobile (java, javascript, activeX)
- Cross-site scripting
- Spoofing email
- Virus envoyés par email
- Extensions de fichiers cachés
- Clients de chat
- Packet sniffing

En dehors de ces risques liés à la connexion à Internet, il existe d'autres risques : crash du disque dur, problèmes électriques, vol, ...

## **4) Se protéger**

Pour se protéger :

- Utiliser un antivirus
- Utiliser un firewall

- Ne pas ouvrir des fichiers joints provenant d'inconnus
- Ne pas lancer un programme d'origine inconnue
- Désactiver les extensions de fichiers cachés
- Garder vos applications et votre système d'exploitation à jour
- Eteindre votre ordinateur lorsque vous ne l'utilisez pas
- Désactiver Java, JavaScript et ActiveX si possible
- Désactiver la gestion des script dans votre logiciel de messagerie
- Faire un backup régulier des données importantes

*Derternet*