

ADMINISTRATION

Journalisation

ADMI02

Contexte :

L'usage des serveurs d'application, et des serveurs d'administration ayant un rôle spécifique (ex. : réseau, sécurité...) exige un enregistrement des événements et des traitements.

Objectifs :

Rendre possible le redémarrage après incident (serveur d'applications), et assurer la traçabilité des événements dans tous les autres cas.

Recommandations :

Généralités

Un journal étant en principe cyclique, il faut définir :

- la périodicité (journalière, hebdomadaire...);
- s'il est cumulatif ou incrémental ;
- les techniques d'élaboration et les procédures
- les moyens pour son exploitation.

Des précautions particulières doivent être mises en œuvre pour éviter que les fichiers journaux soient altérés (volontairement ou non) :

- scellement après sauvegarde du fichier (au minimum par un calcul de checksum) ;
- recopie sur un support « inaltérable » (ex. : CD-ROM...);
- stockage sécurisé selon les mêmes modalités que les sauvegardes, pendant la durée nécessaire (cf. fiche SERV02 sur la sauvegarde);
- accès strictement réservé au(x) administrateur(s) habilité(s) ;

Serveurs d'applications

Les transactions applicatives doivent être gérées par l'administrateur de la base de données qui doit les mémoriser dans un journal d'exploitation (journal " before " ou " after "), afin de les restaurer dans l'état fiable le plus récent, à partir de la dernière sauvegarde.

Autres serveurs

Sous réserve que les performances restent correctes, et que l'on puisse traiter la masse d'information ainsi obtenue, on aura intérêt à activer au maximum les fonctions de journalisation et statistiques.

L'objectif est d'assurer l'auditabilité du système: performances du réseau et des serveurs, connexions et déconnexions, utilisation de ressources, erreurs, anomalies, incidents, détection de programmes malveillants (vers, virus...).

Il est recommandé de centraliser et consolider ces informations vers la ou les consoles de supervision adéquates.

Remarque :

Dans le cas de traitement d'informations à caractère nominatif, l'utilisation de fichiers journaux ou « logs » à des fins d'audit doit être précisée dans la déclaration à la CNIL. La durée de conservation de ces fichiers ne doit pas excéder celle définie par cette commission.



Les présentes recommandations ne sauraient mettre en cause la responsabilité du CLUSIF, elles ne présentent qu'un caractère indicatif et ne sauraient prétendre à l'exhaustivité.