J-EOLE
Recommandations de sécurité pour la mise en œuvre d'un système de journalisation

Emmanuel IHRY

Responsable Pôle National Expertise

serveurs et réseaux

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉGALITÉ DES TERRITOIRES
ET DU LOGEMENT
www.territoires.gouv.fr

MINISTÈRE DE L'ÉCOLOGIE,
DU DÉVELOPPEMENT DURABLE
ET DE L'ÉNERGIE
www.developpement-durable.gouv.fr

Contexte de la présentation

L’ Agence Nationale de la Sécurité des Systèmes d’Information publie des recommandation de sécurité pour la mise en œuvre d’un système de journalisation

Note technique de l'ANSSI du 02/12/2013

- Contexte juridique
- Recommandations de sécurité pour la mise en œuvre d’un système de journalisation

Contexte au MEDDE

Contexte EOLE

Présentation de ZephirLog

Note technique de l'ANSSI

- Aspects juridiques et réglementaires
  - Les éléments juridiques doivent être pris en compte dans le cadre de la conception technique
  - La réglementation pose un principe général d'effacement ou d'anonymisation des données de connexion
  - plusieurs régimes juridiques distincts, notamment
    - Conservation des éléments de journalisation par les fournisseurs d'accès à Internet (FAI) ou d'hébergement – durée = 1 an
    - Conservation des éléments de journalisation des opérateurs de communications électroniques
- Valeur probatoire des éléments de journalisation
  - Objectifs :
    - **permettre la traçabilité de l'activité d'un réseau et d'apporter la preuve de cette activité** (utilisation ou non-utilisation d'une application ou d'un service par un utilisateur, accès illégitime, etc.)
    - **être en capacité à identifier directement ou indirectement un individu ou un équipement ayant participé à cette activité.**
  - Afin d'être **opposable** en cas de contentieux, leur mise en œuvre **doit respecter les règles relatives à l'administration** de la preuve et les principes directeurs des procès civils et pénaux

Document ANSSI
Traces nominatives

- Régime général de protection des données à caractère personnel
  - Les éléments de journalisation peuvent contenir des données à caractère personnel (données relatives à une personne identifiable directement ou indirectement)
  - une adresse de courriel, une URL ou une adresse IP sont régulièrement considérées par la CNIL comme des données à caractère personnel.
- Le traitement d'éléments de journalisation impose le plus souvent le respect des dispositions notamment de la loi du 6 janvier 1978 et en particulier :
  - formalités préalables auprès de la CNIL (déclaration, autorisation, etc.) ;
  - définir une politique claire adaptée aux données traitées et aux finalités ;
  - définir le cycle de vie des éléments de journalisation (processus de création, de conservation, de destruction, etc.) ;
  - respecter les exigences relatives aux droits de la personne
  - ...

Document ANSSI / Aspect juridique
Accès au traces nominatives

- Jurisprudence CNIL
  - seules des personnes spécifiquement habilitées peuvent accéder aux éléments de journalisation ;
  - Ces personnes sont soumises à des obligations de confidentialité particulières
  - l'accès doit être strictement limité à la finalité poursuivie, de la manière la moins intrusive possible pour les données à caractère personnel ;
  - le personnel habilité ne doit subir aucune contrainte quant au dévoilement des informations, notamment par son employeur, sauf si la loi en dispose autrement (dans le cadre d'une procédure judiciaire).
  - Les éléments de journalisation ne peuvent être conservés que pour un temps limité.
  - Les activités liées à la gestion des éléments de journalisation doivent être strictement limitées au but poursuivi.
  - Les procédures liées à la gestion des éléments de journalisation doivent être décrites dans des documents de référence, permettant ainsi de s'assurer que les données à caractère personnel ne sont pas conservées de manière illégitime.

Document ANSSI
Règles de conception technique

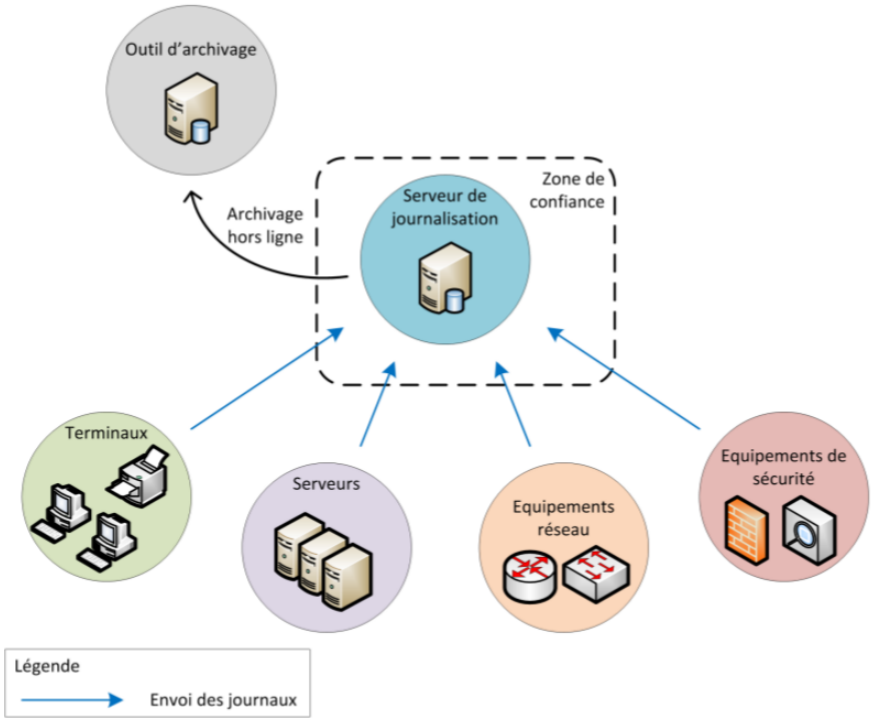
- La prise en compte de la fonction de journalisation est primordiale et doit se faire lors de toute démarche de conception et de développement.
- Les événements doivent être horodatés
  - pour l'ensemble des événements
  - les horloges des équipements doivent être synchronisées
- Dimensionnement
  - l'estimation de l'espace de stockage doit être prise en compte dans le dimensionnement des équipements

Document ANSSI
Règles de conception technique

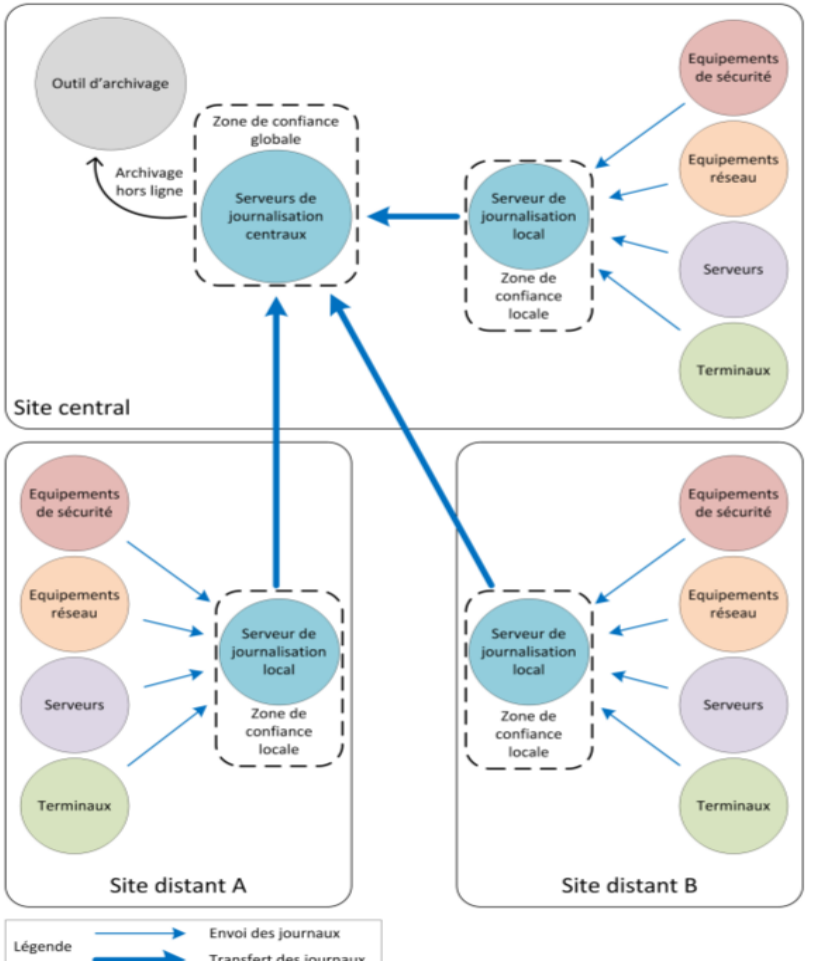
- Recommandations d’architecture et de conception
  - Les journaux doivent être automatiquement exportés sur une machine physique différente de celle qui les a générés.
  - Centralisation sur des serveurs dédiés
  - Redondance nécessaire du serveur central en cas de volume de journaux important ou selon le nombre de site de collecte de journaux
  - Selon la taille ou la typologie du système d’information mise en place d'une approche hiérarchique pour l’organisation des serveurs de collecte.

Architecture de journalisation simple

B.1 Architecture de journalisation simple



Architecture de journalisation étendue/multi-sites



Document ANSSI
Règles de conception technique

- Protection des données échangées
  - Privilégier un transfert en temps réel des journaux sur les serveurs centraux
  - ne pas effectuer de traitement sur les journaux avant leur transfert (peut conduire à dénaturer les évènements et induire des pertes d'information.)
- Fiabilisation du transfert des journaux
  - Il est recommandé d'utiliser des protocoles d'envoi de journaux basés sur TCP pour fiabiliser le transfert de données entre les machines émettrices et les serveurs centraux.

Document ANSSI
Règles de conception technique

- Sécurisation du transfert des journaux
  - utiliser des protocoles de transfert de journaux qui s'appuient sur des mécanismes cryptographiques robustes
  - contrôler la bande passante des flux réseau utilisée pour transférer les journaux d'évènements.
  - En cas de besoin de sécurité, le transfert des journaux doit se faire sur un réseau d'administration dédié.
  - Placer les serveurs de journalisation dans un réseaux spécifique non exposée directement à des réseaux qui ne sont pas de confiance
- Stockage
  - Dédier une partition disque au stockage des journaux d'évènements
  - Prendre en compte les durée réglementaire de stockage.

Document ANSSI
Règles de conception technique

- Protection des journaux
  - L'accès aux journaux doit être limité en écriture à un nombre restreint de comptes ayant le besoin d'en connaître.
  - Les processus de journalisation et de collecte doivent être exécutés par des comptes disposant de peu privilèges.
  - Un outil spécifique doit être utilisé pour une meilleure exploitation des journaux présents sur les serveurs centraux
  - Les comptes ayant accès à l'outil de consultation centralisée des journaux doivent être associés à des rôles prédéterminés.

Contexte MEDDE

- Groupe de travail « optimisation de la gestion des traces nominatives »
  - Acteurs
    - Bureau du droit pénal, du droit privé et de la déontologie
    - Bureau de la sécurité des systèmes d'information
    - Responsables Maîtrise d’œuvre (centre serveurs,PNE)
    - Sous direction de la politique des système d'information
  - Objectifs
    - Actualiser les besoins en terme de gestion des traces nominatives
    - S'assurer de la régularité des besoins vis à vis de la loi

MEDDE / Contrôle des logs de connexion
le cadre juridique ministériel

- Arrêté du 19 juillet 2001 autorisant la création d'un traitement automatisé des journaux d'activité au ministère de l'équipement, des transports et du logement
  - **---> révision en cours d'examen**
  - **---> focus sur la durée de conservation des logs**
- Charte d'utilisation actuelle du réseau internet du MEDDE (octobre 2009)
  - un historique des accès et des actions réalisées par les utilisateurs des SI est conservé, en particulier les traces laissées :
    - sur leur poste de travail et les serveurs bureautiques ;
    - sur les applications informatiques auxquelles ;
    - sur le système de messagerie;
    - sur le système d'accès à Internet lors de l'accès aux sites Web;
    - sur le système de téléphonie.

Contexte EOLE

- Échange autour de ces aspects lors du séminaire technique MEDDE / MEN
- Journaux gérés par les serveurs EOLE
  - journaux système
  - journaux à caractère réglementaires (proxy)
  - manque de structuration, pas toujours facilement exploitables
  - Utilisation de rsyslog, mais pas seulement
  - en 2.3, la possibilité de centraliser les logs existe :
    - Nécessite d'installer un EoleBase et de le configurer afin qu'il reçoive les logs des autres autres machines
- Le Pole Eole propose d'intégrer les recommandations techniques de l'ANSSI dans la distribution EOLE
  - Projet à planifier

FIN

Merci de votre attention

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉGALITÉ DES TERRITOIRES
ET DU LOGEMENT
www.territoires.gouv.fr

MINISTÈRE DE L'ÉCOLOGIE,
DU DÉVELOPPEMENT DURABLE
ET DE L'ÉNERGIE
www.developpement-durable.gouv.fr