

Conservation des Journaux d'Événements sur la solution Hitachi Content Platform®

Hitachi Content Platform (HCP) est la solution Hitachi dédiée à la gestion et l'archivage de documents à contenu fixe. La plate-forme implémente des protocoles d'ingestion, pour la réception et l'organisation automatique de données issues de journaux (logs) et de traces d'activités.

Respectant les exigences de conservation, ainsi que les contraintes d'intégration dans l'entreprise, l'environnement de dépôt WORM logique Hitachi Content Platform incorpore des fonctions de recherche, de sécurisation, de haute disponibilité et de capacité progressive.

Enjeux de la gestion de journaux d'évènements

La journalisation d'évènements est une préoccupation grandissante des entreprises ; celles-ci devant relever des enjeux :

- **Economiques** : le contenu des journaux d'évènements doit être conservé avec un coût-volume contrôlé tout en associant une valeur probante liée à un fonctionnel d'audit. Il faut également maîtriser leur augmentation, leur tri et leur destruction en fin de rétention.
- **Organisationnels** : en rationalisant les flux entrant, afin de favoriser leur consolidation, leur analyse et leur contrôle. La mutualisation permet de réaliser des corrélations au travers d'outil d'indexation de contenu et de recherche multicritères.
- **Réglementaires** : le respect des réglementations, pour la conservation probante et informatisée, doit être réalisé en accord avec les besoins fonctionnels de l'entreprise.
- **Informatique** : les journaux d'évènements sont une source de détection et d'analyse d'incidents, de traçabilité et surtout de sécurité, pour comprendre et interpréter une activité afin d'apporter les corrections préventives sur les causes identifiées.

Principales difficultés

- Duplication non contrôlée des contenus.
- Limite d'extension des capacités de stockage et d'archives.
- Pas de gestion et de mise en relation des contenus.
- Incapacité de recherche performante et de référence croisée.
- Inexistence ou limitation d'assurance qualité.
- Pas de politique formelle d'archivage et de conservation
- Manque d'adéquation avec la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI).
- Inaptitude à évaluer et réduire les risques (ISO 27001).

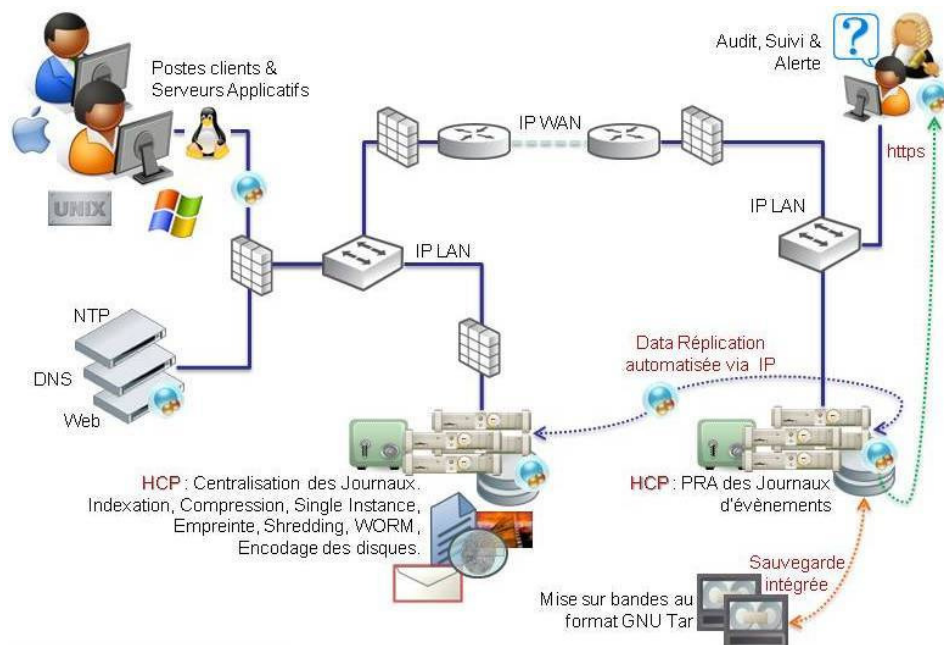
Quelle solution ?

Pour répondre à ces enjeux, Hitachi Content Platform (HCP) apporte l'expérience d'une intégration aboutie matérielle et logicielle, pour la mise en œuvre d'un système simplifié et automatisé de conservation des Journaux avec trie et indexation des contenus multi-formats et multi-langues. Via un simple processus d'envoi de message (email), HCP récupère et ordonne automatiquement les informations avec une gestion des pièces attachées.

Bénéfices

- Solution intégrée logicielle et matérielle de stockage consolidé dédié aux Journaux d'Évènements avec support d'environnements hétérogènes.
- Simplification de la mise en œuvre du Système d'Archivage Electronique avec synchronisation NTP.
- Réduction des coûts et amélioration du retour sur investissement : déploiement, stockage, gestion et interface.
- Conformité de conservation : Accès, Shredding, Audit, WORM (Write Once Read Many), Cnil...
- Indexation et recherche plein-texte sur les contenus, pour une restitution ciblée et sécurisée des contenus avec retours RSS.
- Intégration simplifiée et complète via SMTP avec respect des RFCs 1652, 2821, 2822 et 2920.
- Prêt au support d'extensions en mode SaaS par des solutions logicielles spécialisées.
- Supervision distante du stockage avec SLA (Service Level Objective), plan de reprise d'activité et continuité de service 24/7.

Hitachi Content Platform se charge de recevoir les journaux, de gérer le stockage physique, de protéger, de sécuriser et d'indexer les contenus



- **Une Solution Intégrée et Fonctionnelle** supportant la synchronisation d'horloge (NTP), multi composants (Switch, Routeur, DMZ, etc.), multi plates-formes (Unix, Linux, Windows, Apple, etc.), multi applications (messagerie, SGBD), multi services (Web, DNS, Proxy, etc.) et sans déploiement d'agent propriétaire. HCP réceptionne les messages via le protocole SMTP et effectue une classification automatisée, non propriétaire, par date avec séparation des documents attachés.
- **Une Solution Réglementaire** assurant une conservation immuable, sécurisée, fiable et indispensable à la compréhension et l'historisation du système d'information dans le respect des normes et des standards.
- **Une Solution d'Indexation et de Recherche, pour les Exigences de Métrique et d'Audit**, proposant des interfaces graphiques (https) sécurisées et cloisonnées, pour faciliter la mise en relation d'information issues de plusieurs sources applicatives et informatiques, jusqu'à la mise en œuvre de liens RSS, afin de faciliter au quotidien la lecture d'activités ciblées ou génériques, au plus proche des événements et des alertes de suivi.
- **Une Solution de Diagnostics sur les Archives** qui authentifie (empreinte), trace (journal interne) et garanti l'intégrité des informations sur le temps planifié de conservation (rétention) ; et réalise des suppressions granulaires et effectives (Shredding) des données et métadonnées.

- **Une Solution de Rationalisation des Archives** qui fournit aux organisations des possibilités d'analyse automatisée sur les données et les métadonnées, afin de faciliter la réduction des volumes par la compression et la suppression des doublons (single instance).
- **Une Solution de Protection des Archives** sécurisant les données en local (copie conforme et répartie) et à distance (réplication), et intégrant des procédures automatiques de recouvrement.
- **Une Solution d'Exploitation Performante des Archives** capable de traiter plusieurs dizaines de milliards d'archives dans un seul ensemble de quelques Téra octets à plusieurs dizaines de Péta octets.
- **Une Solution Extensible en Mode SaaS** pour une intégration avec des solutions d'éditeurs logiciels spécialisés dans la gestion de Journaux d'Evènements.
- **Une Solution de Haute Disponibilité 99,999%** au travers d'une architecture GRID Cluster favorisant des évolutions progressives en accord avec les besoins réels et un dimensionnement adapté à toutes les structures d'entreprise. Un support Hitachi distant et automatisé des composants matériels assure une pro activité.



Hitachi Data Systems Corporation – Visitez le centre virtuel Hitachi Content Platform sur <http://vts.hds.com/fr/>

Hitachi est une marque déposée d'Hitachi, Ltd. aux États-Unis et dans d'autres pays. Hitachi Data Systems est une marque déposée et une marque de service d'Hitachi, Ltd. aux États-Unis et dans d'autres pays. Toutes les autres marques de commerce, marques de service et noms de sociétés mentionnés dans le présent document ou site Web appartiennent à leur propriétaire respectif.

Avis : Le présent document est à caractère informatif uniquement et ne stipule aucune garantie, expresse ou implicite, sur aucun équipement ou service offert ou devant être offert par Hitachi Data Systems. Le présent document décrit des fonctionnalités dont les conditions sont définies sur un contrat de maintenance effectif avec Hitachi Data Systems et pouvant dépendre de la configuration, ainsi que des fonctionnalités qui ne sont peut-être pas disponibles actuellement.

Contactez votre revendeur Hitachi Data Systems local pour plus d'informations sur la disponibilité des fonctionnalités et des produits. © Hitachi Data Systems Corporation 2010. Tous droits réservés. 2010. 2 août 2010.