

LOGICIEL EMC DATA DOMAIN ENCRYPTION

Chiffrement sécurisé des données inactives

AVANTAGES CLÉS

Gestion sécurisée des données

- Chiffrement de toutes les données stockées sur un système de stockage avec déduplication Data Domain
- Protection contre le vol ou la perte des données stockées sur le système, les unités de stockage, les disques ou les supports retournés en usine
- Implémentation du chiffrement permettant de respecter les règles de gouvernance internes et les réglementations relatives à la mise en conformité
- Mise en conformité grâce aux algorithmes de chiffrement standard AES 128 ou 256 bits
- Utilisation des bibliothèques de cryptographie validées RSA BSAFE FIPS 140-2

Chiffrement au fil de l'eau

- Chiffrement des données immédiat et en temps réel
- Exploitation de l'architecture SISL pour un chiffrement optimisé
- Contrôle des coûts grâce au chiffrement logiciel

Gestion des clés et intégrité

- Intégration avec RSA Data Protection Manager pour une gestion centralisée du cycle de vie des clés de chiffrement
- Protection optimale contre la perte accidentelle de clés
- Protection des clés de chiffrement par phrase de passe

Intégration simple

- Prise en charge des principales applications de sauvegarde et d'archivage
- Chiffrement des données reçues via EMC Data Domain Boost, VTL, le système CIFS, NFS et NDMP
- Compatibilité avec EMC Data Domain Replicator et le logiciel EMC Data Domain Retention Lock

CHIFFREMENT AVANCÉ DES DONNÉES SAUVEGARDÉES ET ARCHIVÉES

La médiatisation des pertes de données et les nouvelles réglementations relatives à la gouvernance et à la mise en conformité poussent les clients à chiffrer leurs données inactives. Le logiciel EMC® Data Domain® Encryption permet aux entreprises d'améliorer la sécurité de leurs données sauvegardées et archivées, résidant sur leurs systèmes de stockage avec déduplication EMC Data Domain, à l'aide des bibliothèques de cryptographie validées RSA® BSAFE® FIPS 140-2.

Pour de nombreux bureaux de sécurité, la gestion centralisée du cycle de vie des clés de chiffrement est également essentielle. Pour satisfaire cette exigence, vous pouvez utiliser un système Data Domain avec RSA Data Protection Manager, afin de bénéficier d'une solution robuste de gestion du cycle de vie des clés de chiffrement pour l'ensemble de l'entreprise.

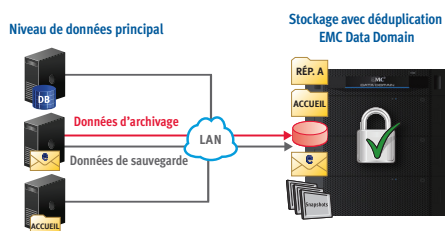
GESTION SÉCURISÉE DES DONNÉES

Le logiciel Data Domain Encryption chiffre toutes les données entrantes pour éviter qu'elles ne soient consultées sur le système existant ou un autre environnement sans authentification et déchiffrement préalables. Le mécanisme de chiffrement des données au repos respecte différents aspects des règles de gouvernance internes et des réglementations relatives à la mise en conformité. Il protège les données utilisateur en cas de vol d'un système Data Domain ou de perte des supports de stockage physiques pendant leur transfert. Il élimine également les risques d'exposition lors du remplacement de disques en panne.

DD Encryption met à disposition des administrateurs les algorithmes AES (Advanced Encryption Standard) 128 ou 256 bits mis en oeuvre par les bibliothèques de cryptographie validées RSA BSAFE FIPS 140-2. Ceux-ci permettent de chiffrer et de déchiffrer toutes les données stockées sur le système. Les modes de chiffrement par blocs de l'algorithme AES peuvent être paramétrés en fonction des règles de sécurité informatique pour garantir la confidentialité via CBC (Cipher Block Chaining), ou pour assurer à la fois la confidentialité et l'authenticité des messages via Galios/Counter Mode (GCM).

CHIFFREMENT AU FIL DE L'EAU

DD Encryption s'intègre de manière transparente avec le processus de déduplication rapide et à la volée utilisé dans les systèmes de stockage avec déduplication Data Domain, et chiffre les données avant qu'elles ne soient écrites sur le disque. À l'instar de la déduplication à la volée, le chiffrement au fil de l'eau nécessite peu de ressources et permet le chiffrement rapide, fiable et sécurisé des données sauvegardées et archivées.



Chiffrement au fil de l'eau d'EMC Data Domain

DD Encryption s'intègre de manière transparente avec le processus de déduplication rapide et à la volée utilisé dans les systèmes de stockage avec déduplication Data Domain, et chiffre les données avant qu'elles ne soient écrites sur le disque. À l'instar de la déduplication à la volée, le chiffrement au fil de l'eau, réalisé pendant l'écriture, nécessite peu de ressources tout en offrant une sauvegarde et une restauration rapides, fiables et sécurisées.

Pour profiter des avantages combinés de la déduplication à la volée et du chiffrement au fil de l'eau, il suffit de demander une licence et d'activer DD Encryption sur le système Data Domain. Le chiffrement au fil de l'eau constitue une solution plus rapide et plus sûre par rapport aux autres options de chiffrement, car les données ne se trouvent jamais dans un état vulnérable et sont toujours chiffrées sur le sous-système de disques.

Contrairement aux autres solutions de chiffrement nécessitant des ressources matérielles supplémentaires ou une puissance de traitement supérieure, DD Encryption ne requiert aucun matériel supplémentaire et n'a qu'un impact minimal sur les performances. L'utilisation de l'architecture évolutive EMC Data Domain Stream-Informed Segment Layout (SISL™) évite le chiffrement des segments en double. Cette optimisation réduit considérablement la consommation des ressources au cours du processus de chiffrement, diminuant ainsi l'impact sur les performances globales et éliminant le recours à des serveurs ou dispositifs supplémentaires dédiés au chiffrement au sein de l'infrastructure.

GESTION DES CLÉS ET INTÉGRITÉ

Par défaut, le logiciel Data Domain Encryption chiffre toutes les données du système à l'aide d'une clé de chiffrement générée en interne. Cette clé est statique et ne peut pas être modifiée par l'utilisateur. Pour les environnements nécessitant la modification périodique des clés de chiffrement afin de satisfaire des exigences de conformité, RSA Data Protection Manager (RSA DPM) permet de gérer le cycle de vie de la clé de chiffrement de chaque système Data Domain. Les règles utilisées pour procéder à la rotation périodique de la clé de chiffrement peuvent être configurées de manière centralisée à l'aide de RSA DPM. Il est également possible de faire expirer les clés, de les supprimer ou de les marquer comme étant compromises lorsqu'il existe un risque de violation de données. Afin de garantir la protection des clés de chiffrement, il est aussi possible de stocker une copie de chaque clé sur un deuxième serveur RSA DPM. En outre, RSA DPM fournit des journaux d'audit répertoriant les modifications apportées à l'état des clés, afin de pouvoir prouver leur conformité.

Pour assurer une flexibilité maximale concernant la sélection de la méthode de chiffrement appropriée, il est possible d'utiliser, dans un même environnement, la clé de chiffrement statique sur certains systèmes Data Domain, tout en exploitant la fonction de rotation des clés de chiffrement via RSA DPM sur d'autres systèmes Data Domain.

Les systèmes Data Domain disposent d'une clé de chiffrement active pour les données écrites sur le système. Pour fournir un niveau de sécurité supplémentaire, une phrase de passe d'accès est utilisée pour crypter la clé de chiffrement lorsque celle-ci est stockée sur le système Data Domain. Les données stockées sur les systèmes Data Domain expédiés peuvent donc être chiffrées et accompagnées d'une clé de chiffrement sans que l'intégrité de cette dernière ne soit altérée.

SIMPLICITÉ D'INTÉGRATION

DD Encryption est compatible avec les principales applications de sauvegarde et d'archivage d'entreprise et s'intègre facilement dans les infrastructures existantes. La flexibilité du déploiement est accrue par la prise en charge de plusieurs méthodes d'accès aux données, utilisables simultanément : Virtual Tape Library d'EMC Data Domain via Fibre Channel, protocoles de service de fichier NFS et ICFS via Ethernet ou cible sur disque, grâce à des interfaces spécifiques des applications telles qu'EMC Data Domain Boost.

DD Encryption simplifie considérablement la gestion du chiffrement, car le processus est effectué sur le système Data Domain en parfaite transparence vis-à-vis des applications écrivant sur le disque. La sélection et la modification des applications gagnent ainsi en flexibilité sans que le processus de chiffrement en pâtisse. En outre, plusieurs applications de sauvegarde et d'archivage peuvent accéder simultanément au système Data Domain.

DD Replicator peut être utilisé avec DD Encryption pour permettre la réplication des données chiffrées sur le réseau. Pour améliorer la sécurité des données transférées sur le réseau, DD Replicator permet le chiffrement des données en cours de transfert. De même, les données de fichier et d'e-mail archivées et sécurisées à l'aide du logiciel EMC Data Domain Retention Lock peuvent également être stockées et répliquées dans un format chiffré.

CARACTÉRISTIQUES TECHNIQUES

LOGICIELS

EMC Data Domain Operating System 4.9 ou version ultérieure (DD Encryption)

EMC Data Domain Operating System 5.2 ou version ultérieure (intégration de RSA Data Protection Manager)

RSA Data Protection Manager 2.7, 3.1

Logiciel EMC Data Domain Boost

Logiciel EMC Data Domain Replicator

Logiciel EMC Data Domain Retention Lock

NOUS CONTACTER

Pour savoir comment les produits, services et solutions d'EMC peuvent vous aider à relever vos défis métiers et informatiques, contactez un responsable de compte ou un revendeur agréé, ou visitez notre site Web à l'adresse www.emc2.fr.

EMC², EMC, Avamar, Data Domain, Global Compression, EMC NetWorker, RSA BSAFE, SISEL et les logos EMC et RSA sont des marques déposées ou des marques commerciales d'EMC Corporation aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans le présent document sont la propriété de leurs détenteurs respectifs. © Copyright 2011-2012 EMC Corporation. Tous droits réservés. 05/12 Fiche produit H7028.4