ORACLE ADVANCED SECURITY

CHIFFREMENT ET MASQUAGE A LA VOLÉE DES DONNÉES A DES FINS DE CONFIDENTIALITÉ OU DE CONTRAINTES RÉGLEMENTAIRES

Oracle Advanced Security apporte au sein de Oracle Database 12c les solutions d'entreprise les plus avancées du marché pour le chiffrement et le masquage à la volée, fonctionnalités vitales pour la protection des données applicatives sensibles. Transparent Data Encryption et Data Redaction permettent de protéger les données sensibles de tout accès non autorisé au niveau applicatif, Operating System, supports de sauvegarde ou exports Oracle. Oracle Advanced Security supporte pleinement l'option 'Oracle Multitenant' et offre des performances inégalées avec les Systèmes intégrés Oracle comme Exadata.

FONCTIONNALITÉS DE CHIFFREMENT

- Chiffrement des données applicatives en base de données (mode colonne ou « tablespace »).
- Gestion du cycle de vie des clés de chiffrement intégrée avec assistance à la rotation des clés.
- Algorithmes standards de l'industrie dont AES (avec clé de 128, 192 ou 256 bits)
- Accélération hardware avec Intel® AES-NI et Oracle SPARC T-Series.
- Intégration avec Oracle Exadata et les technologies Database comme Oracle RMAN, ASM, RAC, Advanced Compression, Active Dataguard et GoldenGate.

FONCTIONNALITÉS DE MASQUAGE

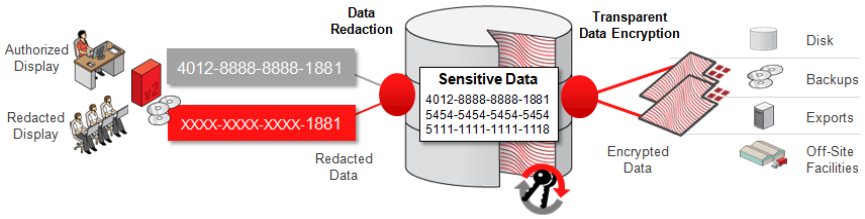
- Masquage à la volée pour limiter l'exposition des données sensibles au sein des applications
- Politiques déclaratives de masquage gérées de façon centralisée dans la Database
- Transformations de masquage multiples avec différents scenarii applicatifs
- Gestion des politiques via Oracle Enterprise Manager et intégrée à Oracle SQL Developer.

BÉNÉFICES CLIENT

- Sécurité des données cohérente de façon transparente pour l'ensemble des applications existantes (spécifiques et progicielles)
- Implémentation rapide
- Facile à déployer et à administrer
- Support complet de l'option Oracle Multitenant

Aperçu d'Oracle Advanced Security

La protection de données exige une approche de type 'défense en profondeur' comprenant des contrôles préventifs, de détection ou administratifs. Les contrôles préventifs d'Oracle Advanced Security permettent d'adresser de nombreuses exigences de type réglementaire, de limiter les risques de violation de données et de protéger les données privatives. Par exemple, les données liées à des cartes de paiement peuvent être chiffrées automatiquement sur disque et en même temps masquées à la volée avant de quitter la base de données dans le cadre d'un résultat de requêtes SQL. Ces deux fonctionnalités sont essentielles pour obtenir une conformité sur les données privatives et respecter le standard de sécurité des données de cartes de paiement (PCI-DSS).



Transparent Data Encryption

Transparent Data Encryption (TDE) protège les données sensibles de tout accès non autorisé depuis l'extérieur de l'environnement base de données en chiffrant ces données sur le support où elles sont stockées. Les utilisateurs OS à privilèges non autorisés ne peuvent plus accéder directement aux données sensibles en inspectant le contenu des fichiers de données ('datafiles'). TDE protège aussi contre la perte ou le vol de media de stockage contenant des exports ou backups de base de données.

La solution est transparente pour les applications car les données sont automatiquement chiffrées lors de l'écriture sur disque et déchiffrées lors d'une lecture. Les contrôles d'accès mis en place au niveau de la base de données sont toujours en vigueur. Les requêtes SQL ne sont jamais altérées et aucune modification de code ni de configuration n'est nécessaire.

Le processus de chiffrement et déchiffrement est extrêmement rapide car TDE bénéficie des optimisations des mécanismes de cache Oracle. TDE exploite aussi l'accélération hardware des architectures basées sur Intel® AES-NI et Oracle SPARC T-Series (Oracle Exadata et SPARC SuperCluster notamment). Enfin, TDE bénéficie des avantages de 'Exadata Smart Scan' (déchiffrement rapide et en parallèle dans les multiples cellules de stockage) et de 'Exadata Hybrid Columnar Compression' (réduction importante du nombre d'opérations de cryptographie nécessaires).

PRODUITS CONNEXES

Les produits suivants complètent l'offre Oracle Database 12*c* Defense-In-Depth Security :

- Oracle Database Vault
- Oracle Audit Vault and Database Firewall
- Oracle Data Masking
- Oracle Label Security

TDE est basé sur une architecture de clés de chiffrement à deux niveaux comprenant des clés de chiffrement de données et des clés de chiffrement maître. Les clés maître sont stockées à l'extérieur de la base de données dans un 'Oracle Wallet' (fichier chiffré normé PKCS) ou dans un périphérique externe sécurisé (HSM). Des fonctionnalités intégrées de gestion de clés permettent une assistance à la rotation des clés sans rechiffrement des données et une gestion de leurs cycles de vie.
TDE peut être déployé très facilement. Il est installé par défaut avec la base de données. Les données existantes peuvent être chiffrées sans arrêt de service sur les systèmes de production en utilisant 'Oracle Online Table Redefinition' ou bien en mode offline lors d'une fenêtre de maintenance. Bien sûr, TDE fonctionne en standard avec 'Oracle Automatic Storage Management' (ASM).

Masquage à la volée de données avant visualisation

Data Redaction permet de masquer une sélection de données sensibles avant de les afficher au sein d'une application afin que seules les personnes autorisées ne puissent visualiser ces données sensibles, ceci en préservant un masquage cohérent des colonnes de bases de données pour tous les modules applicatifs accédant aux mêmes informations. Data Redaction n'implique aucun changement dans les applications car aucune donnée n'est modifiée dans les buffers et les caches internes, ni dans les données stockées sur disque. Les types de données et formats originaux sont préservés par le masquage à la volée, ainsi l'application ne subit aucune perturbation. Data Redaction n'a aucun impact sur les activités opérationnelles database comme les backups, restores, upgrades, patchs et clusters haute disponibilité.

Contrairement aux approches historiques basées sur du codage applicatif et de nouveaux composants logiciels, les politiques de Data Redaction sont appliquées directement au niveau du noyau de la base de données. Les politiques déclaratives peuvent contenir différents types de transformations (partielles, aléatoires, ou générées suivant un modèle). Le masquage peut être conditionnel et dépendre de différents facteurs connus de la base de données ou transmis à la base de données par les applications (identifiant de l'utilisateur, signature de l'application ou adresses IP du client par exemple). Une bibliothèque de méthodes de masquage fournit un choix des modèles préconfigurés de colonnes pour les types de données sensibles les plus communs (N° carte de crédit ou N° SS par exemple). Une fois activées, les politiques de masquage sont appliquées immédiatement y compris pour les sessions déjà actives.

Protection des données de l'entreprise

TDE et Data Redaction sont faciles à administrer dans le cadre d'une stratégie de sécurité de type 'défense en profondeur'. Oracle Enterprise Manager propose une console d'administration simple et efficace ; une API en mode ligne de commande est également disponible.
TDE et Data Redaction complètent les autres fonctionnalités database tout en étant parfaitement intégrés avec les outils Oracle les plus fréquemment utilisés. Par exemple, le chiffrement en mode tablespace de TDE fonctionne de manière transparente avec Oracle Recovery Manager (RMAN) afin d'effectuer des backups compressés et chiffrés.
Oracle Advanced Security supporte pleinement l'option 'Oracle Multitenant'. TDE et Data Redaction restent actifs lorsque les 'pluggable databases' sont déplacées vers un nouveau container et ainsi protègent les 'pluggable databases' même en transit.