

SecureSphere®

Passerelle de contrôle de bases de données

Contrôle de l'activité opérationnelle automatisé, audit et reporting pour bases de données



Les réglementations gouvernementales et les normes de l'industrie conduisent les organisations à étendre les processus d'audit à l'information sensible stockée au sein des bases de données. Les auditeurs et les professionnels des nouvelles technologies (IT) doivent collaborer afin de prouver que l'usage des données dans la Suite Oracle E-Business (EBS), SAP, PeopleSoft et les applications métier propriétaires répondent aux exigences de contrôle SOX et autres réglementations. L'activité de l'administrateur de bases de données (DBA) doit être contrôlée activement et comparée aux politiques organisationnelles et aux contrôles.

Malheureusement, l'audit des applications cruciales et des bases de données n'est pas une mission simple. Celles-ci servent une large variété d'utilisateurs avec des privilèges différents pour chacun, supportent des taux de transactions importants et doivent répondre à des exigences de niveau de service élevées. Les capacités d'audit intégrées dans les logiciels commerciaux de bases de données ne répondent pas aux besoins fondamentaux d'indépendance, dégradent la performance des bases de données et augmentent les coûts d'administrations. Les produits d'audit tiers, en revanche, ne pistent pas toute l'information demandée par les auditeurs. SecureSphere est une solution complète d'audit, indépendante, qui satisfait aux exigences de conformité en préservant la performance des applications.

Passerelles de contrôle de bases de données SecureSphere®.

Les passerelles de contrôle de bases de données (SecureSphere Database Monitoring Gateways) font partie de la famille des dispositifs d'audit automatisés de bases de données pour les environnements Oracle, MS-SQL, IBM DB2 (y compris gros systèmes), Sybase, et Informix. Déployées en contrôleurs de réseau non en ligne, les passerelles SecureSphere effectuent un enregistrement indépendant et détaillé de l'activité des toutes les applications de bases de données avec une attention particulière pour les applications packagées telles qu'Oracle E-Business Suite, SAP et PeopleSoft. Un agent hôte dédié permet également le contrôle de l'activité locale (par exemple : console, telnet, ssh, IPC, et mémoire partagée) des administrateurs de bases de données. Bien que SecureSphere puisse être déployé comme dispositif autonome, un serveur d'administration centralisé permet la gestion unifiée des passerelles et agents distribués.

Points forts de SecureSphere

- Le pistage universel de l'utilisateur (Universal User Tracking) relie l'activité des bases de données aux utilisateurs connectés via les serveurs d'application et les connexions regroupées.
- Le Profilage Dynamique crée automatiquement les profils vérifiés de l'activité utilisateur et identifie les variances substantielles.
- L'architecture d'audit distribuée permet la collecte de données détaillées en préservant l'extensibilité.
- L'audit unifié des environnements mixtes MS-SQL, Oracle, DB2, Sybase, et Informix automatise l'intégration des logs multi-fournisseurs.
- Le déploiement du dispositif réseau et de l'agent hôte local assurent le contrôle de l'ensemble de l'activité des bases de données.
- Le déploiement transparent (Transparent deployment) simplifie l'implémentation sans impact sur la performance des bases de données ou leur disponibilité.

Contrôle de l'activité et audit

Responsabilisation utilisateur

L'objectif principal de tout audit de base de données consiste à valider que la responsabilisation utilisateur a été établie. Un audit compatible SOX, par exemple, doit consigner chaque changement dans les données de reporting financier avec un identifiant unique (premier/dernier, nom utilisateur, etc.) De nombreuses solutions d'audit de bases de données ne répondent pas à cette exigence, qui se situe au-delà des scénarios d'authentification les plus basiques.

La technologie de surveillance universelle de l'utilisateur (Universal User Tracking) de SecureSphere rend les utilisateurs individuels responsables dans tous les scénarios d'authentification en combinant de multiples méthodes d'identification. Les comptes utilisateur de bases de données et les adresses IP sources identifient les administrateurs de bases de données (DBA) avec des droits d'accès direct aux requêtes. Les noms hôtes OS et noms utilisateurs identifient les utilisateurs des comptes root aux privilèges partagés. Les transactions de bases de données sont corrélées avec les logins des applications Web et les sessions pour surveiller les utilisateurs qui s'authentifient et sont ensuite agrégés sous un seul compte utilisateur (regroupement de connexions). Enfin, SecureSphere applique des algorithmes personnalisés pour identifier les utilisateurs qui s'authentifient via des applications métier multi-niveaux telles que SAP, et Oracle EBS.

Profil utilisateur vérifié et variances substantielles

Les auditeurs exigent des organisations de suivre les variances substantielles du comportement normal d'accès autorisé. Cette tâche est souvent considérable, étant donné que la vision de base de chaque comportement utilisateur autorisé n'est pas disponible.

Afin de répondre au besoin d'identification des variances substantielles, la technologie du Profilage Dynamique de SecureSphere applique des algorithmes d'apprentissage sophistiqués

données sensibles, évaluation de configuration, et évaluation de comportement. Ensemble, ces capacités fournissent l'information nécessaire pour définir la configuration de base et l'usage de la date, identifier les risques, évaluer toutes les actions correctives éventuelles ou atténuer les contrôles, et documenter la conformité.

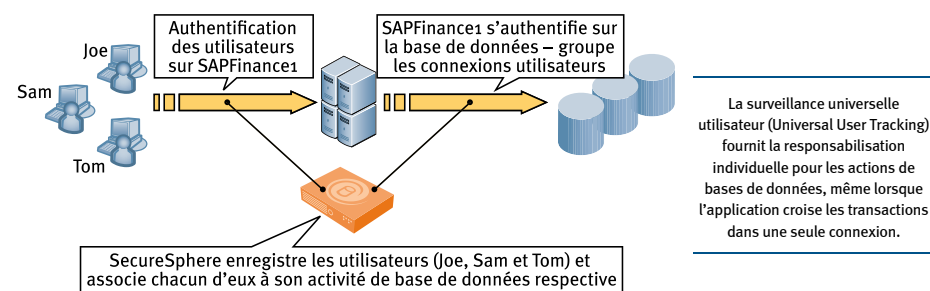
La technologie d'identification de données sensibles (Server & Sensitive Data Discovery) simplifie la découverte des données sensibles. SecureSphere balaye d'abord une gamme d'adresses IP de réseau pour déceler l'existence de tous les serveurs d'applications Web et de bases de données. Ensuite, il peut scanner au sein de chaque base de données pour rechercher des données sensibles telles que les numéros de cartes bancaires, les numéros de sécurité sociale, les numéros de cartes nationales d'identité, etc. Même les données cryptées peuvent être identifiées et contrôlées.

L'évaluation de configuration émet des requêtes pour la recherche d'informations sur la configuration, y compris la conformité avec plus de 350 tests de sécurité, et d'autres informations sur les caractéristiques importantes de la base de données. La procédure de test couvre des domaines clés tels que les privilèges utilisateurs, la configuration logicielle, les défaillances logicielles connues, les objets externes, et la conformité aux bonnes pratiques.

L'évaluation de comportement identifie les vulnérabilités qui peuvent être seulement identifiées en contrôlant l'activité au cours du temps. Par exemple, les événements de login sont analysés au cours du temps pour détecter les comptes utilisateur partagés par de multiples utilisateurs - une violation de sécurité claire mise en exergue par la plupart des infrastructures de contrôle IT.

Indépendance et séparation des tâches

Afin d'assurer l'intégrité, l'audit devrait être indépendant du serveur de bases de données et séparer les tâches d'audit de l'administration de la base de données. Par exemple, un audit qui



pour créer et maintenir automatiquement des profils de base vérifiés pour chaque comportement utilisateur normal. Le personnel responsable de la conformité compare ensuite les profils aux fonctions, exigences réglementaires ou bonnes pratiques. Les profils peuvent être éventuellement modifiés, approuvés, et convertis en politiques autorisées appliquées par SecureSphere pour identifier automatiquement les variances substantielles au cours du temps.

Évaluation complète

SecureSphere fournit trois capacités uniques d'évaluation distinctes : identification des

se base sur des capacités d'audit intégrées peut être facilement compromis par un administrateur malhonnête qui désactiverait les fonctions d'audit.

SecureSphere permet la séparation des tâches entre les fonctions d'audit et d'administration de base de données. Il peut être déployé sans privilège, sans modification de configuration des bases de données, et mis en œuvre par le personnel opérationnel de sécurité ou d'audit sans connaissances particulières en administration de bases de données.

Opérations

Détails et évolutivité

L'architecture de l'audit distribué de SecureSphere permet à la fois la journalisation détaillée et l'extensibilité au niveau de l'entreprise. L'architecture distribue la collecte de l'audit, le stockage des données et le traitement analytique aux multiples passerelles DMG à haute performance. Le serveur d'administration de SecureSphere présente des visuels de haut niveau de l'audit à partir d'une console unifiée. Lorsque les responsables de la conformité ont besoin d'approfondir les visuels jusqu'aux détails des logs, le serveur d'administration fournit automatiquement l'information à partir des passerelles distribuées.

Pour répondre aux exigences de traitement de très grands ensembles de données et de conservation des données sur le long terme, l'information de l'audit peut être périodiquement archivée sur des serveurs externes. Afin de préserver l'intégrité des données et réduire les contraintes de stockage, les données archivées peuvent être cryptées, signées et compressées. L'accès aux données archivées est contrôlé à partir de l'interface de visualisation d'audit SecureSphere.

Définition souple de la politique d'audit

L'assistant de la politique d'audit de SecureSphere permet la spécification des critères d'audit en quelques minutes. Une règle peut spécifier le pistage complet de toutes les transactions de données sensibles, ou le pistage sélectif sur la base d'une combinaison d'attributs (voir Tableau d'audit SecureSphere). De plus, des règles multiples peuvent être opérées pour suivre les accès aux données depuis différentes perspectives. Par exemple, une règle concernera tous les accès à une table spécifique, pendant qu'une autre ne portera que sur les changements de table. Les services ADC Insight fournissent des règles extrêmement ciblées, des évaluations, des rapports et plus encore, pour des applications et exigences spécifiques.

Reporting intelligent

Une solution d'audit générique qui se contente simplement de la journalisation de montagnes de transactions de base de données, ne répond pas aux questions d'audit spécifiques concernant les bonnes pratiques des différentes industries, applications, réglementations et infrastructures. Les données doivent être analysées et présentées aux auditeurs dans un format pertinent par rapport aux spécificités de chaque entreprise.

La solution de reporting graphique de SecureSphere intègre tous les outils analytiques

nécessaires pour documenter la conformité avec la pertinence adaptée aux environnements métier spécifiques. L'ensemble des rapports de conformité "prêts à l'emploi" le plus complet du marché accélère l'audit par rapport à la gamme des cadres réglementaires/des bonnes pratiques, dont SOX, HIPAA et PCI. Ces rapports concernent non seulement des critères réglementaires spécifiques mais des critères pertinents pour les applications telles que SAP et Oracle EBS. Aucune autre solution de base de données ne fournit la capacité "prêt à l'emploi" de se concentrer sur les questions d'audit spécifiques de réglementation et d'applications métier.

Le reporting de SecureSphere supporte également la programmation, la personnalisation et l'exportation de données vers des outils de reporting externes.

Couverture complète avec le contrôle local de base de données

L'agent de contrôle de sécurité d'administrateur (SecureSphere DBA Monitor Agent) surveille toute l'activité des bases de données en local/sur console. La surveillance de l'agent ne comprend pas seulement l'activité via console, telnet et ssh, mais aussi l'activité via mémoire partagée/IPC Ensemble, l'agent de contrôle (SecureSphere DBA Monitor Agent) et les dispositifs réseau assurent la couverture de l'activité des bases de données via n'importe quelle méthode d'accès aux bases.

Réponse en temps utile

La plupart des systèmes d'audit sont limités à l'analyse post-mortem des événements de bases de données. Les alertes en temps réel de SecureSphere permettent une réponse immédiate aux variances, si souhaité. Les politiques d'alerte granulaires peuvent être configurées d'une manière souple pour une gamme de variances comprenant les violations de profils utilisateur, les tentatives d'évasion d'audit, les opérations SQL privilégiées, et les violations de politique de contrôle d'accès réseau. Même les corrélations spécifiques de ces variances peuvent déclencher des alertes.

Déploiement

Déploiement Transparent

SecureSphere est déployé de façon transparente comme contrôleur réseau sans impact sur l'infrastructure IT. Il ne nécessite aucun changement dans le réseau, les applications,

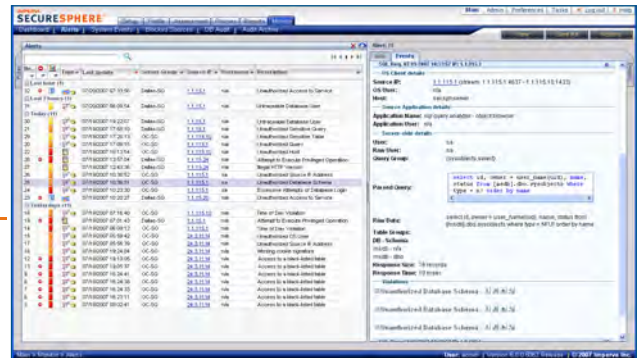
Services ADC Insight – Connaissance métier

En plus des passerelles (SecureSphere Database Gateways), Imperva offre des services uniques ADC Insights - un audit prédéfini, un contenu de sécurité et de conformité qui vous maintient à jour avec la connaissance approfondie la plus récente des applications spécifiques telles que SAP et Oracle EBS, des risques liés à ces applications et des obligations réglementaires comme SOX, PCI et HIPAA. ADC Insights fournit aussi des modèles sur la base des normes de sécurité de l'industrie et des bonnes pratiques nécessaires afin de répondre aux défis de sécurité, conformité et audit.

ou bases de données ; il n'a aucun impact sur la performance des bases de données ; et il n'introduit aucun point de défaillance.

Gestion centralisée

SecureSphere peut être déployé comme dispositif autonome ou distribué au sein d'importants centres de données. Pour les grands environnements, le serveur d'administration (SecureSphere Management Server) fournit une configuration, un contrôle et un reporting centralisés. La gestion est standardisée via des regroupements hiérarchiques organisationnels (clients, unités d'affaires, lieux, etc.), des droits d'accès granulaires basés sur les rôles, et un workflow unique orienté-tâches d'administration.



SecureSphere contrôle tous les accès aux bases de données ainsi que toute l'activité y survenant. Les rapports prêts à l'emploi permettent d'identifier rapidement l'activité non autorisée et l'adhésion aux exigences réglementaires.

Information d'audit SecureSphere – Contrôle en profondeur de l'activité

Utilisateur	Nom utilisateur de base de données, Application Web Nom utilisateur, nom utilisateur OS source, groupe utilisateur
Données	Base de données, schéma, table, colonne
Opérations	Toutes opérations SQL – DML, DDL, DCL, procédures stockées
Requête	Texte de requête, groupe de requêtes, texte de réponse, taille de réponse, temps de réponse, codes de réponse, chaînes de code de réponse
Programmes	Déclarations préparées, requêtes dynamiques et imbriquées, procédures stockées et opérations exécutées
Contexte	Date, temps, OS source, application source, URL source, nom hôte source, lieu utilisateur, lieu base de données
Variances/Alertes	Profil, configuration dans les règles de l'art, comportement de bonnes pratiques, fuites de données, tentatives d'évasion d'audit (violation de protocole/IPS), opérations SQL privilégiées

Spécifications du dispositif SecureSphere

Spécifications	SecureSphere G4	SecureSphere G8	SecureSphere G16 FTL
Production	500 Mbit/s	1000 Mbit/s	2000 Mbit/s
Transactions SQL/Sec	50 000	100 000	200 000
Latence	Inférieure à la milliseconde	Inférieure à la milliseconde	Inférieure à la milliseconde
Interfaces	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)	6 x 10/100/1000 Mbit/s (max 4 interfaces fibre)
Types d'interfaces	Cuivre/Fibre SX/Fibre LX	Cuivre/Fibre SX/Fibre LX	Cuivre/Fibre SX/Fibre LX
Segments Max	5	5	5
Unité de rack	1U ; Modèle FTL 2U	1U ; Modèle FTL 2U	2U
Disque dur	250GB SATA ; Modèle FTL (2) Hot-Swap 250GB SATA	250GB SATA ; Modèle FTL (2) Hot-Swap 250GB SATA	(2) Hot-Swap 250GB SATA
Disque externe	CD-ROM	CD-ROM	CD-ROM
Taille de rack	Rack 19 pouces (483 mm)	Rack 19 pouces (483 mm)	Rack 19 pouces (483 mm)
Poids	11.34 Kg ; Modèle FTL 29.48 Kg	11.34 Kg ; Modèle FTL 29.48 Kg	29.48 Kg
Alimentation	350W Modèle FTL (2) Hot-Swap 750W SATA	350W Modèle FTL (2) Hot-Swap 750W SATA	(2) Hot-Swap 750W SATA
Puissance AC	100-240V 50-60 FTL	100-240V 50-60 FTL	100-240V 50-60 FTL
Dimensions	430 mm x 648 mm x 42 mm Modèle FTL 430 mm x 705 mm x 87 mm	430 mm x 648 mm x 42 mm Modèle FTL 430 mm x 705 mm x 87 mm	430 mm x 705 mm x 87 mm
Environnement opérationnel	10°C (50°F) à 35°C (95°F)	10°C (50°F) à 35°C (95°F)	10°C (50°F) à 35°C (95°F)
Environnement non opérationnel	-40°C (-40°F) à 70°C (158°F) relative humidité 90%, sans condensation à 35°C (95°F)	-40°C (-40°F) à 70°C (158°F) relative humidité 90%, sans condensation à 35°C (95°F)	-40°C (-40°F) à 70°C (158°F) relative humidité 90%, sans condensation à 35°C (95°F)
Certifications EMC	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI

Spécifications	Serveur d'administration MX
Unité de rack	1U ; Modèle de tolérance de pannes : 2U
Interfaces	2 x 10/100/1000 Mbits/s cuivre
Disque dur	250GB SATA ; Modèle de tolérance de pannes : (2) permutable à chaud 250GB SATA
Lecteur de disque	CD-ROM
Taille de rack	Rack 19 pouces (483 mm)
Poids	11.34 Kg ; Modèle FTL 29.48 Kg
Alimentation	350W SATA ; Modèle de tolérance de pannes : (2) permutable à chaud 750W SATA
Puissance AC	100-240V 50-60 FTL
Dimensions	430 mm x 648 mm x 42 mm ; Modèle FTL 430 mm x 705 mm x 87 mm
Environnement opérationnel	10°C (50°F) à 35°C (95°F)
Environnement non opérationnel	-40°C (-40°F) à 70°C (158°F) relative humidité 90%, sans condensation à 35°C (95°F)
Certifications EMC	FCC, CISPR 22, CE, VCCI

Imperva Inc.

Siège social aux États-Unis
950 Tower Lane
Suite 1550
Foster City, CA 94404
Tél : +1-650-345-9000
Tél : +1-650-345-9004

Siège social international
125 Menachem Begin Street
Tel-Aviv 67010
Israël
Tél : +972-3-6840100
Tél : +972-3-6840200

Numéro vert (États-Unis seulement) : +1-866-926-4678
www.imperva.com

© Copyright 2008, Imperva, Inc.
Tous droits réservés. Imperva et SecureSphere sont des marques déposées d'Imperva, Inc.
#DS-DMG-0308_FR

