Assure Monitoring and Reporting

Puissant audit de l'activité du système IBM i et des bases de données

Face à la complexité des exigences réglementaires et à l'évolution des menaces qui pèsent sur les activités des entreprises, vous avez besoin d'un moyen simple de contrôler toute l'activité des systèmes et des bases de données IBM i, d'identifier rapidement les écarts par rapport aux bonnes pratiques en matière de conformité ou de sécurité et de conserver une piste d'audit pour satisfaire les responsables de la sécurité et les auditeurs.

Assure Monitoring and Reporting, un module d'Assure Security, faisant parti de l'ensemble de fonctionnalités Assure Compliance Monitoring, surveille de manière exhaustive l'activité des systèmes et des bases de données afin de vous faire gagner du temps et économiser lors de la mise en conformité réglementaire, de l'identification des écarts de conformité et de détection des activités non autorisées sur les systèmes IBM i.

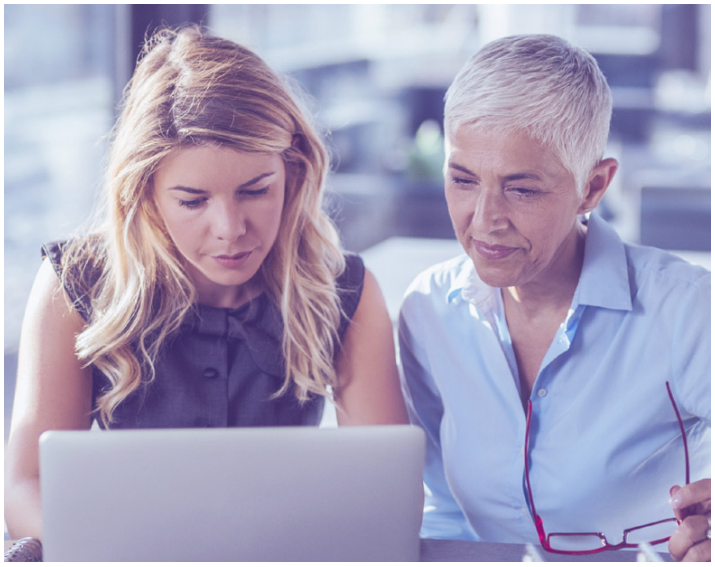
Assure Monitoring and Reporting produit des rapports clairs, concis et faciles à lire, basés sur l'activité du système et les modifications de la base de données enregistrées dans les journaux - la seule source d'informations d'audit acceptée par les professionnels de la sécurité et de l'audit d'IBM i. De plus, aucune modification de l'application n'est nécessaire.

Les rapports peuvent être ad hoc ou programmés et envoyés automatiquement par courrier électronique aux personnes qui en ont besoin. Assure Monitoring and Reporting peut, en option, s'intégrer à une console SIEM pour surveiller les événements de la base de données, les événements ou les informations du système avec d'autres systèmes de l'entreprise.

Assure Monitoring and Reporting est composé de deux modules, le module System et le module Database, qui peuvent fonctionner indépendamment ou ensemble. Le module System d'Assure Monitoring and Reporting surveille votre système de manière exhaustive afin d'établir des rapports sur les modifications apportées aux objets du système, les tentatives d'accès, l'activité des utilisateurs puissants, l'activité de la ligne de commande, l'accès aux données sensibles, et bien plus encore. Le module Database produit des rapports et des alertes pour toute activité autour des bases de données sur l'IBM i.

Avantages

- Simplifie le processus d'analyse des journaux complexes
- Réduit le temps et les dépenses nécessaires à la mise en conformité avec les réglementations GDPR, SOX, PCI DSS, HIPAA, etc.
- Surveillance complète de l'activité du système et de la base de données
- Identifie rapidement les incidents de sécurité et les écarts de conformité lorsqu'ils se produisent
- Répond aux exigences d'une piste d'audit basée sur un journal
- Favorise la séparation des tâches et renforce l'indépendance des auditeurs.



Les sources de données statiques du système sont également analysées pour identifier les écarts possibles par rapport aux meilleures pratiques.

Aucun environnement n'est trop petit ou trop grand et complexe pour bénéficier de la puissance et de la flexibilité qu'offre Assure Monitoring and Reporting pour la surveillance et le reporting de la sécurité et de la conformité d'IBM i.

Fonctionnement d'Assure Monitoring and Reporting

L'objectif d'Assure Monitoring and Reporting est d'extraire uniquement les données pertinentes des journaux afin que les administrateurs puissent se concentrer sur les informations utiles. Une fois les journaux enregistrés dans Assure Monitoring and Reporting, un référentiel de champs est généré pour permettre l'analyse des entrées du journal et la sélection des champs à auditer. Sur la base de ce référentiel, des requêtes peuvent être définies pour générer des rapports d'audit.

Les modules Database et System d'Assure Monitoring and Reporting utilisent tous deux des requêtes pour définir et générer un rapport.

Une requête spécifie des détails tels que :

- La source d'information (journal de la base de données, journal du système ou informations système)
- Les règles d'analyse et le type de rapport qui définissent exactement ce qui doit être vérifié et inclus dans le rapport
- Le format du rapport.
- Niveau de détail du rapport et règles de présentation
- Le mode de distribution du rapport (courriel, IFS ou message SIEM)
- La destination ou la liste des utilisateurs qui recevront le rapport généré

Lors de l'exécution d'une requête, un processus est lancé qui analyse les écritures ou les informations système, extrait les informations correspondant aux règles d'analyse, génère un rapport d'audit avec les résultats d'analyse formatés et le distribue.

Les rapports peuvent être exécutés en continu, selon un calendrier ou à la demande. Le mode continu vous informe en temps réel des événements au fur et à mesure qu'ils se produisent.
Ceci permet d'identifier rapidement les actions malveillantes ou les défauts nuisibles.

Avec Assure Monitoring and Reporting, vous pouvez facilement produire des rapports sur des activités telles que :

- Les accès aux fichiers en dehors des heures de travail
- Les accès aux champs sensibles de la base de données, tels que les numéros de compte bancaire ou de carte de crédit
- Les modifications d'un champ qui dépassent une limite, par exemple une modification de plus de 10 % d'une limite de crédit.
- Tous les accès à partir d'une adresse IP, d'un port, d'un travail ou d'un utilisateur spécifique.
- Activité de la ligne de commande pour les utilisateurs puissants (*ALLOBJ, *SECADM)
- Les modifications apportées aux objets du système, tels que les valeurs du système, les profils d'utilisateur et les listes d'autorisations
- Tentatives de connexion à un compte spécifique ou d'accès à un objet spécifique
- Actions sur un fichier spool sensible, telles que l'affichage ou la suppression du fichier spool de paie
- les transferts d'objets vers les bibliothèques de production et les répertoires IFS.

Caractéristiques principales

- Facile à installer et à configurer
- Ne nécessite aucune modification de l'application
- N'a pas d'impact sur les applications
- Compatible avec les solutions de haute disponibilité
- Audite l'activité du système et de la base de données
- Analyse tout type d'entrée de journal, y compris QAUDJRN, QACGJRN, QZMF, les entrées utilisateur, etc.
- Examine les sources statiques telles que les objets QSYS.LIB ou IFS, les profils, les valeurs système, les listes d'autorisations, les commandes, les travaux, les fichiers spool, etc.
- Fournit un moteur de requête puissant avec un filtrage étendu
- Génère des rapports et des alertes en continu, selon un calendrier ou à la demande
- Fournit des rapports d'audit prédéfinis pour les applications ERP courantes.
- Fournit un modèle prêt à l'emploi pour l'évaluation de la conformité au RGPD
- Production de rapports aux formats PDF, XLS, CSV et PF
- Prise en charge de la distribution des rapports via SMTP, FTP ou l'IFS
- Permet de personnaliser les rapports PDF en y ajoutant des logos, en mettant en évidence les changements, etc.
- Offre des notifications d'événements ou des alertes par e-mail, popup ou syslog
- S'intègre en option avec les principales consoles du marché.