Air France s'appuie sur Oracle pour sécuriser la paie de 60 000 salariés

Avec près plus de 60 000 employés, Air France est le premier employeur privé d'Ile-de-France. En 2014, le groupe lance son projet de paie sécurisée, visant à protéger ces données contre toute consultation par des personnes non habilitées, et contre le piratage. *«Une confidentialité qui s'étend aussi aux administrateurs de bases de données,»* précise Patrick Vergne, manager Database Linux (Engineering & Support) chez Air France. *«Il s'agissait de mettre en place un processus de sécurité en adéquation avec l'organisation de l'entreprise.»*

Une informatique à la taille de l'entreprise

Dans une si grande entreprise, l'organisation multiforme de la DSI permet de s'organiser selon les besoins et les métiers. D'autant plus qu'elle est commune pour Air-France et KLM. Six directions se partagent les tâches et responsabilités informatique: CIO-office, développement, systèmes distribués, opérations, contrôle de gestion IT et RH.

Dans les bureaux et les trois datacenters répliqués en local (Nice, Toulouse et Amsterdam), de multiples technologies cohabitent : Linux, zOS, OS/2200, Windows Server, VMware et Hyper-V, SAP, Oracle, Postgresql, MySql, Db2, Teradata, Hadoop, MongoDB, Splunk, SiteMinder… Et les volumes sont à la hauteur avec 1 500 serveurs (Linux/Unix) pour 1 900 VMs et 1,1 pétaoctet de données. A elles seules les bases de données (hors SAP) sont stockées sur 140 Serveurs pour 1 500 bases totalisant 140 téraoctets.

L'entreprise n'a pas attendu ce projet pour adresser la problématique bases de données/sécurité. Le support est d'ailleurs agencé en 4 niveaux d'escalade: le help-desk (pilotage H24), le service desk (H24 pour serveurs, applications/middleware/BDD, stockage et sécurité), le service Engineering et Support, et en dernier lieu le support des éditeurs.

Sécuriser la paie, préserver la confidentialité

La paie fonctionne sous HR Access, utilisée par 300 utilisateurs, pour l'édition de bulletins de paie, les virements bancaires et la gestion des documents légaux. Soit 350 heures de traitements par mois, majoritairement en batch.

Le projet de sécurisation est organisé en deux lots. Après une phase de conception et de réalisation d'architecture technique, le premier lot est réalisé en août 2014, et en production dès mars 2015. Le second lot initié mi-aout 2015 est mis en production mi-décembre.
Pour la DSI, *«il était primordial de maintenir autant que possible les mêmes tâches d'administration courante que sur les autres bases de données,»* souligne Patrick Vergne.

Après études de solutions et projet pilote, Air France a finalement retenu le logiciel Oracle Database Vault. *« La solution répondait à nos attentes pour sécuriser les environnements de recette de qualification et*

de production, de contrôle précis d'accès aux données (interrogation, mises à jour, etc.), de maîtrise de la copie ou du déplacement de données, et de gestion fine et ciblée pour les audits », précise le manager.

Point sensible, le contrôle d'attribution des comptes et des privilèges s'étend jusqu'à la limitation précise des attributions de chaque compte d'administration. *«Certes, cet aspect est toujours délicat, mais les administrateurs de bases de données savaient qu'il fallait en passer par là,»* confirme Patrick Vergne.

Dès le départ, l'équipe complète Oracle Database Vault, pour le combiner avec Oracle Transparent Encryption (OTE). En effet, si le premier propose quelques fonctions de chiffrement, OTE apporte le chiffrement systématique des tablespaces applicatifs, et la gestion locale des clés de chiffrement.

Une gestion maîtrisée des exceptions

« La recette et la mise en production ont été réalisées sur des bases de données dédiées à partir d'un environnement préconfiguré. Une frustration nécessaire pour les administrateurs afin de favoriser l'approche empirique consistant à n'ouvrir la sécurité que de façon justifiée et documentée,» rapporte Patrick Vergne.

En « régime de croisière", la sécurité est portée à son "maximum acceptable". Dans une politique de sécurité efficace, les contrôles et autres limitations génèrent immanquablement des contraintes. Cependant, des phases spécifiques autorisent une ouverture temporaire de droits ou encore des audits. *«Les équipes DBA communiquent avec l'équipe de sécurité, qui exécute un ensemble de scripts pour ouvrir et fermer les droits,»* détaille le manager. *«En cas d'opération imprévue, un workflow est mis en place pour fluidifier la communication et favoriser la réactivité.»*

Un ressenti positif partagé

Les administrateurs de ces deux outils apprécient la grande souplesse de l'outil pour écrire les règles. Ces spécialistes doivent disposer de connaissances DBA, et garder un œil critique sur les aspects sécurité. Avec le recul, les équipes d'Air France estiment que la solution est stable dans le temps.

« Côté applications, Database Vault et Transparent data Encryption sont assez transparents. Dans notre utilisation, nous ne constatons pas de dégradation notable de performances ni d'impact sur le code applicatif. En revanche, il y a quelques impacts sur l'optimisation des performances. Finalement, les DBA s'y font très bien avec le temps,» rapporte Patrick Vergne, qui conclut: *«En 2016, nous mettrons en place l'externalisation des traces/log sous Splunk, et des opérations de tentatives d'intrusion dans le cadre d'audit de l'infrastructure.»*

A lire aussi :

Bases de données : Oracle plus que jamais leader, percée du NoSQL

Oracle accusé par la FTC de tromperie sur la sécurité de Java SE

Crédit Photo : Hans Engberg-Shutterstock