EVIDIAN

A Groupe Bull Company

Gérer efficacement les identités et les accès

Réconciliation, automatisation de processus et politique d'accès basée sur les rôles

Livre blanc

2013

39 F2 13LV 00

Gérer les identités et les accès

Ce livre blanc explique comment faire évoluer votre gestion des identités et des accès (‘identity and access management’ ou IAM) au-delà de la simple automatisation de processus. En effet, les solutions d’IAM permettent maintenant de baser votre politique de sécurité sur les rôles des utilisateurs, tout en la réconciliant avec l’utilisation réelle de l’informatique.

Pour la plupart des entreprises, gestion des identités est synonyme d’administration des comptes applicatifs. Mais comment des outils techniques peuvent-ils relayer les politiques de sécurité définies au niveau du management de l’entreprise ? Comment les projets d’IAM peuvent-ils dépasser l’automatisation de processus pour mettre en place cette politique et en garantir l’efficacité ?

La réconciliation est un moyen efficace pour unifier les projets d’IAM et faire en sorte que la sécurité soit respectée dans l’ensemble de l’entreprise.

Rendre l’IAM efficace pour vous

Les projets d’IAM réussis sont basés sur des objectifs pratiques et rationnels. Ces objectifs poussent les décideurs à approuver un projet, le financer et le mener jusqu’à son terme.

- **Objectifs de conformité :** de nombreuses lois et règlements exigent que les entreprises fonctionnent dans le respect de règles. Certaines lois sont valables dans tout secteur, notamment les lois sur l’intégrité du reporting financier (comme Sarbanes-Oxley). D’autres sont spécifiques à une activité, par exemple les normes pharmaceutiques ou les lois sur la confidentialité des soins de santé (décret de confidentialité en milieu hospitalier). Mais la plupart d’entre elles nécessitent la mise en place de contrôles et de politiques d’intégrité, de confidentialité ou de disponibilité.

- **Objectifs de réduction des coûts :** les organisations rationalisent leurs procédures en raison d’une pression financière constante. L’IAM peut être d’une grande aide pour alléger la charge de main d’œuvre des processus récurrents. À son tour, l’allègement des tâches courantes manuelles permet de mettre en place des stratégies plus ciblées.

- **Objectifs de flexibilité :** rendre les employés productifs où qu’ils se trouvent, et mettre en œuvre rapidement les décisions opérationnelles. Aujourd’hui, l’informatique favorise la mise en application des objectifs business car elle permet de déployer en quelques heures un nouvel outil, accessible aux utilisateurs internes et externes à l’entreprise.

Le point de départ : l'automatisation des processus

Le principal défi de l'IAM aujourd'hui n'est pas tant lié aux fonctions de base qu'aux objectifs, à l'exécution et à l'intégration des projets.

La plupart des projets mono-fonction d'IAM visent à automatiser des processus sous une forme ou une autre. Maintenir une politique de sécurité avec des outils de suivi, automatiser l'administration des comptes grâce au provisionnement, gérer les mots de passe par une authentification unique... Tous ces projets se concentrent sur l'automatisation de tâches manuelles.

Domaine du projet d'IAM	Projet typique	Motivation business principale	Promoteurs du projet
Rôles	▪ Role mining ▪ Outil de définition de politiques	Conformité aux lois et règlements	Contrôle interne Direction générale
Identités	▪ Provisionnement des utilisateurs ▪ Consolidation d'annuaires	Simplification de l'informatique et réduction des coûts	Direction informatique
Accès	▪ Authentification unique (SSO) ▪ Authentification forte	Flexibilité business et réduction des coûts	Utilisateurs Direction sécurité

L'automatisation des processus est une nécessité vitale pour la plupart des entreprises. À mesure que les systèmes d'informations deviennent de plus en plus complexes, le coût de l'autorisation manuelle augmente de façon exponentielle.

- **Hétérogénéité** : la mise à jour manuelle des comptes dans des dizaines de types de systèmes différents requiert planification et ressources. Souvent, les administrateurs compétents sont réticents à effectuer ces tâches subalternes. C'est particulièrement vrai dans le cas des applications anciennes.

- **Organisation et processus** : lorsqu'un employé change de poste, comment déterminer les systèmes dans lesquels il doit avoir de nouveaux comptes, et éliminer les comptes obsolètes ? Les processus manuels sont souvent basés sur le bouche à oreille et mal documentés. Et quand l'utilisateur quitte l'entreprise des années plus tard, ses comptes ne sont pas supprimés, car personne n'a documenté leur création.

- **Évolution historique des politiques** : de nombreuses entreprises se sont développées via des acquisitions et ont été réorganisées... Or le département informatique est censé garder la trace des demandes d'autorisation. Des travaux « archéologiques » sont souvent nécessaires pour reconstituer des profils d'utilisateur cohérents.

En conséquence, les projets d'IAM qui remplacent les tâches manuelles en automatisant des processus offrent généralement un excellent retour sur investissement. Mais sont-ils suffisants ?

Vers une politique stratégique d'IAM

Les projets mono-fonction « d'automatisation de processus » sont incontestablement utiles. Mais leur véritable potentiel réside dans leur capacité à fonctionner ensemble. La raison en est simple : comme pour d'autres domaines de l'entreprise, une politique de sécurité informatique efficace se structure typiquement autour de contrôles. Ainsi, les auditeurs vérifieront les trois domaines suivants :

1. Un ensemble de contrôles doit **exister**. Pour la sécurité informatique, il s'agit principalement du domaine de la gestion des politiques : qui peut accéder à quoi, et dans quelles circonstances ?
2. Ces contrôles doivent être **appliqués**. Et un bon moyen de le faire consiste à automatiser les politiques de sécurité informatique via le provisionnement ou le workflow. Cela a pour effet de réduire l'impact des erreurs humaines.
3. Une fois mis en œuvre, ces contrôles doivent être **efficaces**. Ici, la gestion des accès garantit que seules les personnes autorisées peuvent accéder aux ressources définies lors des phases précédentes. Et cela peut être vérifié à tout moment au niveau central.

Toutefois, il n'est souvent pas simple de faire fonctionner tous les éléments de l'IAM ensemble et de façon coordonnée :

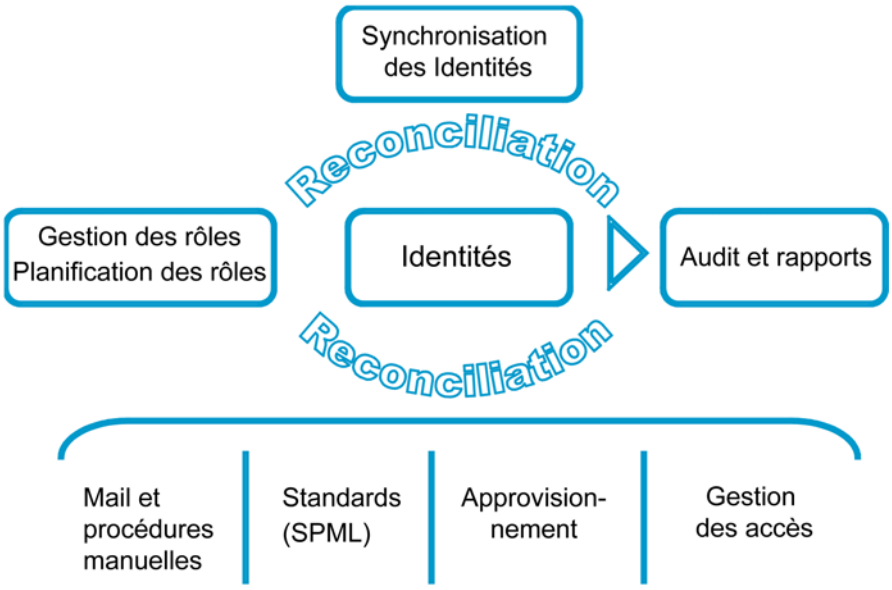
- **Défis de planification** : les projets doivent être mis en attente si certaines fonctions ne sont pas suffisamment modulaires. Par exemple, des projets de SSO sont parfois retardés par un projet de provisionnement associé – alors qu'ils pourraient très bien progresser en parallèle.
- **Défis techniques** : certains modules ne sont simplement pas conçus pour fonctionner ensemble. D'importants travaux d'intégration s'avèrent alors nécessaires.
- **Défis humains** : différentes organisations ont parrainé et gèrent les différentes pièces du puzzle IAM. Une fois formalisées et auditées, les procédures résultantes ne devraient plus être modifiées inutilement. Même pour un projet d'intégration.

Comment alors construire un système d'IAM efficace, pas à pas, et sans perdre de vue l'objectif global ? Pour relever ces défis, Evidian a intégré avec succès les différents éléments d'IAM en utilisant des processus de réconciliation.

La réconciliation : résoudre le puzzle de l'IAM

Pour qu'un système d'IAM complet fonctionne de façon cohérente, Evidian a constaté que la réconciliation est le concept fédérateur le plus efficace. Grâce à la réconciliation incrémentale, l'ensemble de l'infrastructure d'IAM reste gérable à l'échelle humaine. Cela facilite également l'audit, car chaque étape est documentée.

Avec la réconciliation, chaque domaine est géré par les personnes les plus compétentes. Par exemple, les répertoires d'identité sont gérés par le département des RH et les comptes applicatifs par le service informatique. Chaque organisation accepte à l'avance l'étendue et les limites de la réconciliation, ainsi que la manière dont ses propres données seront affectées.



Réconciliez vos sources d'identité

Dans de nombreuses entreprises, les informations d'identité sont hétérogènes et partielles : répertoires locaux, bases de données de RH, systèmes téléphoniques, etc. Comment disposer d'un seul référentiel d'identité fiable ? La solution d'Evidian réconcilie les différentes sources d'identité, en prélevant dans chacune d'elles les éléments les plus fiables. Ainsi, elle crée et met à jour une base de référence des identités des utilisateurs : c'est une condition indispensable pour la plupart des projets d'IAM.

Réconciliez votre politique avec les comptes informatiques

Comment vous assurer que les droits d'accès à vos ressources reflètent votre politique de sécurité ? La plupart des applications ont une multitude de comptes par défaut, comptes partagés et autres accès mal définis. En réconciliant votre politique avec vos comptes, vous pourrez documenter, expliquer ou éliminer les disparités. Les comptes sont ensuite modifiés avec le provisionnement des utilisateurs d'Evidian, de façon manuelle ou automatique.

Réconciliez votre politique avec l'usage réel de l'informatique

La réconciliation des comptes n'est qu'un aspect du problème. Comment faire en sorte qu'il n'existe pas de comptes orphelins ou que les employés utilisent bien les comptes créés à leur intention ? Les utilisateurs qui accèdent aux comptes de leurs collègues présentent un danger sérieux pour une entreprise. La solution de gestion des accès d'Evidian surveille et contrôle l'accès aux ressources critiques. Elle vous aide à réconcilier votre politique avec l'utilisation réelle de l'informatique.

Evidian : gestion des rôles basée sur la réconciliation

Définissez et appliquez facilement votre politique de sécurité

Comment concevoir une politique d'accès aux applications efficace et contrôler son application ? La gestion des rôles d'Evidian unifie l'administration de vos droits d'accès tout en automatisant le circuit d'autorisation.

Comment vous conformer simplement aux nouvelles contraintes légales ?

Vous devez formaliser et surtout, appliquer vos procédures d'attribution de droits d'accès tout en surveillant leur efficacité. La gestion des rôles d'Evidian est la tour de contrôle de votre politique de sécurité.

- **Une politique claire** : Les droits d'un employé dépendent de son rôle, de son entreprise, de son emplacement, etc. Ainsi, sa politique d'accès est alignée sur ses tâches réelles.
- **Une maintenance aisée** : Tous les composants d'une politique de sécurité sont définis à l'aide d'un seul outil. Cela simplifie la documentation et la mise à jour des procédures.
- **Des audits facilités**: Les audits sont plus rapides puisqu'ils sont réalisés depuis un emplacement unique. Vos indicateurs de qualité sont fiables et publiés régulièrement.

Votre politique est rédigée... mais est-elle appliquée ?

Avec la gestion des rôles d'Evidian, votre politique est réellement appliquée. Un workflow automatise la prise de décision - de l'approbation des droits à la création de comptes. Les administrateurs peuvent confirmer si une action a été réalisée ou non.

La fonction de réconciliation d'Evidian vérifie régulièrement et automatiquement votre politique et la compare à la réalité du terrain. Ainsi, les utilisateurs et les décideurs se conforment naturellement à votre politique de sécurité.

Comment prenez-vous en compte les droits existants ?

Au cours des dernières années, vous avez déployé différentes politiques de sécurité. Ces politiques doivent être prises en compte, mais comment savoir quels droits existent encore ? Avec le gestionnaire de politique d'Evidian, vous utilisez la gestion des accès pour concevoir votre politique de sécurité en fonction des accès réels des utilisateurs.

La réconciliation aligne l'utilisation de l'informatique sur votre politique

La gestion des rôles d'Evidian assure que votre politique est respectée. Elle utilise la réconciliation pour comparer régulièrement votre politique aux comptes applicatifs et à leur utilisation réelle.

- Réconciliez votre politique avec les comptes d'utilisateur existants

La gestion des rôles d'Evidian compare les comptes déduits de votre politique avec les comptes existants. Elle le fait avec le provisionnement des utilisateurs d'Evidian ou d'autres solutions de provisionnement. Ensuite, vous pouvez décider de mettre à jour vos applications ou votre politique de sécurité afin d'être aussi proche que possible de la réalité du terrain.

- Réconciliez votre politique avec l'authentification unique (SSO) de l'entreprise

Les administrateurs utilisent les données d'accès réel pour concevoir et valider votre modèle. Vous pouvez détecter quelles personnes utilisent un compte donné. Ainsi, votre politique est affinée par l'analyse des disparités.

Les valeurs ajoutées de Evidian Role Management

1. **Gérez le cycle de vie complet des droits d'accès**.

Dès l'instant où un employé arrive dans un département et jusqu'à son départ de l'entreprise, la gestion des rôles d'Evidian gère ses droits d'accès et les circuits d'autorisation. Vos utilisateurs sont immédiatement productifs tout en respectant la politique de sécurité.

2. **Utilisez la réconciliation pour baser votre politique d'accès sur la réalité du terrain**.

La gestion des rôles d'Evidian compare l'état souhaité des droits avec les accès réellement effectués et les comptes applicatifs existants. Ainsi, votre politique est en phase avec les activités quotidiennes de l'entreprise.

3. **Utilisez la réconciliation pour faire respecter votre politique de sécurité**

Les managers valident officiellement leurs actions et leurs décisions en quelques clics de souris. La fonction de réconciliation vous permet d'appliquer en permanence votre politique. L'audit est simple car il est centralisé.

Evidian IAM Suite est une solution modulaire et intégrée de gestion des identités et des accès. Ses composants permettent aux entreprises de gérer les identités, les rôles et les accès, notamment l'authentification unique (SSO). Ses modules peuvent être déployés individuellement et apportent l'ensemble des fonctions d'IAM par des processus de réconciliation.

Pour plus d'informations, consultez le site www.evidian.com/

Email: info@evidian.com

Livre blanc

EVIDIAN
A Groupe Bull Company