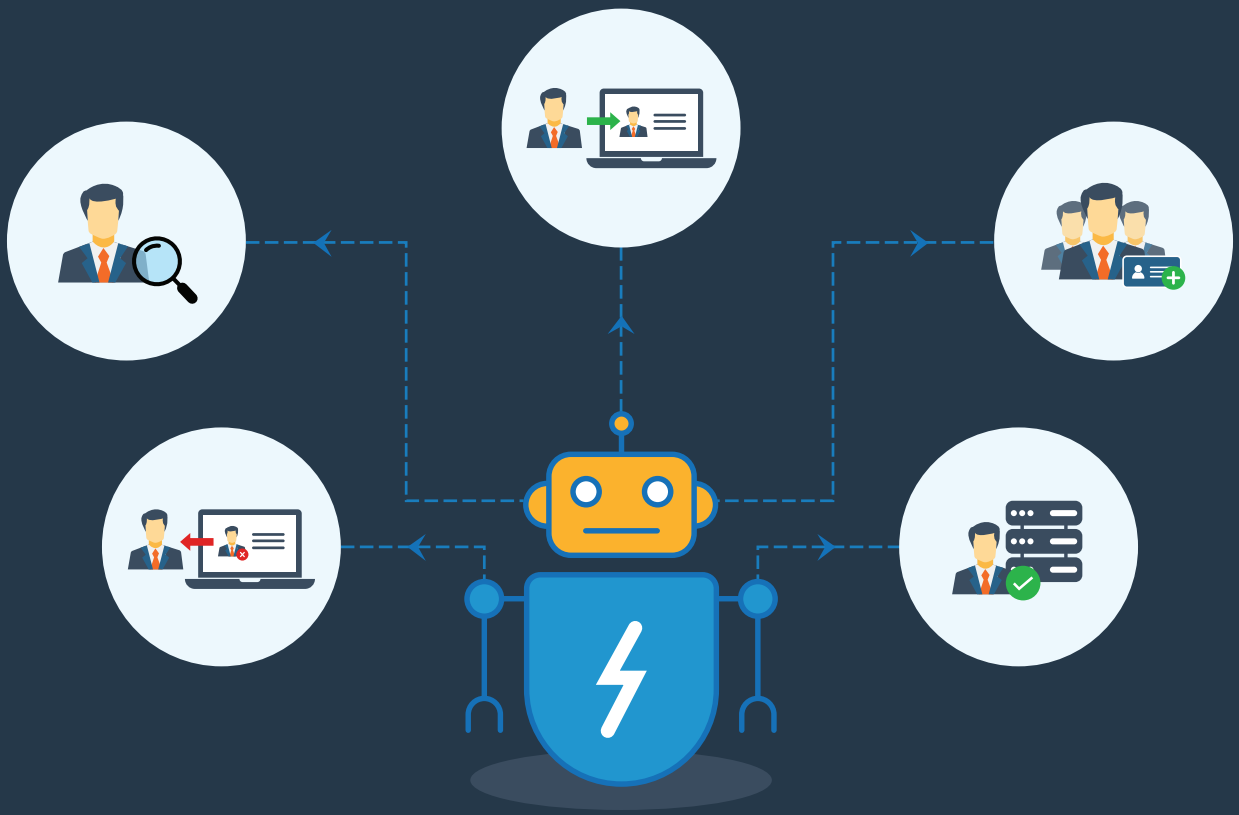
ManageEngine
ADManager Plus

5 raisons pour lesquelles vous devez automatiser le processus IAM



https://www.pgsoftware.fr/iam/admanager-plus

L'IAM est un cadre essentiel pour la sécurité et la conformité, car il définit les identités et les privilèges des utilisateurs au sein d'une entreprise. Cependant, même une simple erreur IAM peut entraîner des risques pour la sécurité des informations d'une entreprise. En raison de la nature précaire d'Active Directory (AD), les techniciens et administrateurs informatiques effectuent souvent manuellement des tâches fastidieuses de gestion des utilisateurs à l'aide d'outils AD natifs, de PowerShell et d'autres méthodes inefficaces.

Pour les entreprises qui se développent chaque jour, l'exécution manuelle de ces tâches de gestion des utilisateurs devient fastidieuse. De plus, certaines tâches AD cruciales, telles que l'approvisionnement et le désapprovisionnement des utilisateurs et la gestion des licences Office 365, ne laissent aucune place à l'erreur. Ce guide expose les erreurs les plus courantes en matière de gestion des identités et de contrôle des accès, et explique en quoi l'automatisation est la meilleure solution pour éviter ces erreurs.

1. Délai d'exécution élevé lors de l'intégration de l'utilisateur.

Comment le service RH informe-t-il les administrateurs informatiques lorsque de nouveaux employés rejoignent l'entreprise ? Dans la plupart des cas, le responsable RH exporte les informations utilisateur dans un fichier CSV à partir de son application SGHR et partage le fichier avec l'équipe informatique par e-mail. La création de comptes utilisateur dans AD et la définition des droits d'accès pour chacun d'entre eux prennent beaucoup de temps et peuvent entraîner des erreurs de saisie, qui peuvent ensuite conduire à l'octroi de droits d'accès inappropriés aux utilisateurs. L'automatisation de la provisioning des utilisateurs élimine les tâches répétitives liées à l'intégration, ce qui libère beaucoup de temps aux administrateurs informatiques pour se consacrer à d'autres tâches importantes.

ADManager Plus permet d'intégrer des comptes utilisateurs en masse et sans intervention dans AD, Office 365, Exchange, Skype for Business et G Suite en utilisant des modèles basés sur des règles personnalisables. Vous pouvez également configurer ADManager Plus pour qu'il récupère automatiquement les derniers détails de l'utilisateur et provisionne les comptes à partir des bases de données SGRH telles que MS SQL, Oracle et d'autres applications SGRH populaires.

2. Réponse retardée en raison d'un trop grand nombre de demandes de modification de la part des utilisateurs.

Lorsque les rôles ou les responsabilités des employés changent, l'administrateur doit modifier les propriétés de leurs comptes, les ajouter aux groupes appropriés ou les déplacer vers une autre unité organisationnelle. Les administrateurs doivent immédiatement traiter les appartenances à des groupes et les autorisations d'accès aux serveurs de fichiers, car celles-ci déterminent l'accès des employés aux ressources pertinentes. De plus, les administrateurs sont constamment sollicités pour réinitialiser des mots de passe, déverrouiller des comptes et répondre à d'autres demandes d'assistance. Tout retard dans le traitement de ces demandes de modification nuit à la productivité des employés et de l'équipe. Vous pouvez effectuer des actions de gestion groupée à l'aide d'outils natifs, mais uniquement via des scripts PowerShell complexes.

ADManager Plus offre une variété d'actions automatisées de modification des utilisateurs, notamment la réinitialisation des mots de passe et la redistribution des licences Office 365. ADManager Plus vous aide également à informer les utilisateurs concernés par e-mail ou SMS chaque fois qu'une action de gestion est effectuée.

3. Accumulation de comptes périmés.

Les comptes orphelins peuvent passer inaperçus pendant longtemps, et se débarrasser des comptes obsolètes est une bonne stratégie de sécurité. Il est important de supprimer ces comptes des systèmes dès que possible afin d'éliminer les attaques potentielles d'anciens employás mácontents ou de personnes malveillantes au sein de l'entreprise. Dans un scénario non automatisé, lorsqu'un employé quitte l'organisation,le service des ressources humaines ou l'ancien responsable de l'employé demande à l'administrateur de supprimer le compte. Cependant, le processus de suppression peut souvent prendre du temps, voire ne jamais avoir lieu. En automatisant le nettoyage des comptes AD, vous empéchez efficacement les anciens employés qui souhaiteraient accéder aux données de l'entreprise d'y parvenir.

ADManager Plus simplifie la suppression des comptes en identifiant automatiquement les comptes obsolàtes, en les retirant de leurs groupes, en les dáplaÜant vers une autre unitá organisationnelle et en les dásactivant ou en les supprimant conformáment à la politique de votre entreprise.

4. Les utilisateurs ont des droits excessifs.

Parfois, les administrateurs accordent des privilèges supplémentaires aux utilisateurs pour accéder à des serveurs de fichiers critiques à des fins spécifiques, telles que l'audit, et oublient de révoquer ces privilèges une fois leur objectif atteint. Les utilisateurs disposant de droits excessifs peuvent avoir accès à des informations classifiées, qui pourraient être volées. La mise en place d'un environnement sécurisé dans lequel les utilisateurs de confiance se voient temporairement accorder des autorisations d'accès à certains fichiers, dossiers et groupes peut être un moyen infaillible de garantir que les utilisateurs ne disposent que des droits nécessaires.

ADManager Plus redéfinit la gestion des accès privilégiés grâce à l'attribution automatique des utilisateurs à des groupes de sécurité de niveau supérieur pour une période donnée. En outre, vous pouvez utiliser des rapports NTFS prédéfinis pour identifier les utilisateurs qui accèdent aux ressources critiques de votre environnement.

5. Impossible de suivre les actions de gestion effectuées à l'aide de PowerShell ou ADUC.

Les administrateurs n'ont pas de visibilité sur les actions de gestion des utilisateurs effectuées à l'aide des outils traditionnels, car ceux-ci ne permettent pas de prévisualiser les modifications dans AD ni de détecter les modifications non autorisées. Vous pouvez améliorer la visibilité des actions de gestion AD en mettant en oeuvre un workflow automatisé.

ADManager Plus offre une automatisation contrôlée, qui garantit que chaque tâche automatisée est examinée et approuvée par un responsable ou un utilisateur approprié avant d'âtre exécutée.

ADManager Plus álimine les risques, les tracas et les coóts liés à la gestion manuelle du cycle de vie des comptes utilisateurs dans les entreprises en pleine croissance. Outre les actions de gestion des utilisateurs, l'outil offre une gamme d'actions de gestion automatisées prédéfinies pour les contacts, les ordinateurs et les groupes AD.

Nos produits

AD360 | Log360 | ADAudit Plus | ADSelfService Plus | M365 Manager Plus | RecoveryManager Plus

ManageEngine
ADManager Plus

ManageEngine ADManager Plus est une solution Web de gestion et de reporting Windows AD qui aide les administrateurs AD et les techniciens du service d'assistance à accomplir leurs tâches quotidiennes. Grâce à son interface intuitive et facile à utiliser, ADManager Plus gère une multitude de tâches complexes et génère une liste exhaustive de rapports AD, dont certains sont indispensables pour satisfaire aux audits de conformité. Il aide également les administrateurs à gérer et à générer des rapports sur leurs environnements Exchange Server, Office 365 et G Suite, en plus d'AD, le tout à partir d'une seule console.

Pour plus d'informations sur ADManager Plus, rendez-vous sur
https://www.pgsoftware.fr/iam/admanager-plus

$ Cotation ⬇ Télécharger