

Présentation

ADManager Plus

novembre 2023

Présentation ADManager Plus

Solution de gestion et de suivi Active Directory (AD) qui permet aux administrateurs et aux techniciens informatiques de gérer facilement les objets AD et de générer des rapports instantanés d'un seul clic.

1/ Gestion

1.1 : Création en masse d'utilisateurs Active Directory

L'un des grands défis auxquels fait face un administrateur informatique réside dans la création en masse d'utilisateurs Active Directory. Les outils natifs Active Directory (AD) ou les scripts PowerShell sont très chronophages pour attribuer chaque compte d'utilisateur et configurer leurs propriétés dans AD.

La solution Web ADManager Plus permet de créer plusieurs utilisateurs dans AD et d'autres environnements comme Office 365, Exchange, Google Workspace et Skype Entreprise, le tout dans une seule console. Grâce à elle, lorsqu'on crée des comptes d'utilisateur dans AD, on peut aussi créer des boîtes aux lettres Exchange et des comptes dans Office 365, Google Workspace, et Skype Entreprise.

Flux de création en masse d'utilisateurs

1.2 Gestion des utilisateurs Active Directory en bloc

La gestion des comptes d'utilisateurs dans Microsoft Active Directory est un défi pour chaque administrateur informatique. La configuration manuelle des propriétés de l'utilisateur à l'aide des outils de l'Active Directory natif ou d'autres options comme PowerShell, etc., est extrêmement chronophage, fastidieuse et source d'erreurs, en particulier dans un réseau Windows vaste et complexe. De plus, des connaissances approfondies sur Active Directory et la gestion Active Directory sont absolument nécessaires pour accomplir ces tâches.

ADManager Plus est un logiciel Web qui vous permet de créer et gérer plusieurs comptes d'utilisateurs dans Active Directory en une seule action. En outre, grâce à ce logiciel, vous pouvez aussi créer des boîtes aux lettres Exchange, de comptes d'utilisateurs dans Office 365 et G Suite également pour tous les utilisateurs désirés, au moment précis où vous leur créez de nouveaux comptes dans Active Directory. Il vous permet de créer plusieurs modèles qui contiennent des valeurs d'attribut d'utilisateur standard, qui peuvent être appliqués lors de la création d'utilisateurs en bloc. Vous pouvez importer les attributs d'utilisateur depuis un fichier CSV unique pendant que vous créez les comptes d'utilisateurs, en réduisant ainsi au minimum le temps et les efforts nécessaires lorsque les outils natifs sont utilisés pour l'approvisionnement des utilisateurs Active Directory. Vous pouvez même exporter des utilisateurs avec une facilité absolue à l'aide de cet outil qui fait également office de logiciel de gestion des autorisations Windows.

Cet outil permet aussi de déléguer les droits aux techniciens du service d'assistance ou aux utilisateurs non-administrateurs de créer des utilisateurs. Avec cette délégation, vous aurez largement le temps de vous consacrer à des tâches essentielles, étant donné que vous serez

libéré des tâches répétitives et triviales. Grâce à la réactive des comptes d'utilisateurs, vous pouvez même gérer plusieurs attributs de comptes d'utilisateurs en une seule étape. En outre, cette fonctionnalité vous permet même de définir des règles pour configurer ou mettre à jour automatiquement certains attributs d'utilisateur pendant que vous exécutez des tâches de gestion d'utilisateur. De plus, avec la fonctionnalité de génération automatique de rapports, vous pouvez gérer non seulement les comptes d'utilisateurs, mais aussi l'intégralité d'Active Directory de manière proactive et efficace.

À l'aide d'ADManager Plus, vous pouvez modifier en masse les attributs d'utilisateur, notamment les attributs Exchange Server (2003/2007/2010/2013) et les stratégies appliquées, les attributs Lync Server/LCS/OCS et Services Terminal Server. Vous pouvez essayer toutes les fonctionnalités de gestion des utilisateurs et même de création de rapports offertes par ce logiciel à l'aide de la version d'évaluation ; son téléchargement est gratuit et elle fournit un accès illimité à l'ensemble des fonctionnalités. Diverses fonctions courantes de gestion, d'administration et de modification d'attributs dans Active Directory peuvent être exécutées rapidement et régulièrement :

- Créer un compte d'utilisateurs pour plusieurs utilisateurs
- Modifier les attributs de plusieurs utilisateurs
- Réinitialiser les mots de passe de plusieurs comptes d'utilisateurs
- Modifier le nom d'affichage de l'utilisateur
- Créer une boîte aux lettres Exchange et appliquer les stratégies Exchange
- Créer des comptes Office 365 et G Suite
- Activer/désactiver/supprimer les comptes inactifs dans AD
- Déplacer les utilisateurs entre les différentes unités organisationnelles
- Gestion automatisée des utilisateurs en bloc
- Gestion mobile des utilisateurs Active Directory

1.3 Gestion des mots de passe Active Directory

ADManager Plus intègre les fonctions suivantes pour faciliter la gestion des mots de passe Active Directory :

- Réinitialisation de mot de passe unifiée pour Active Directory, Exchange Server, Office 365, Google Workspace et Lync/OCS.
- Réinitialisation de mot de passe en masse via un fichier CSV.
- Gestion de la sécurité à la volée à partir de rapports intégrés sur les mots de passe.
- Option de définir simultanément des mots de passe uniques pour plusieurs utilisateurs.
- Modification de mot de passe régulière automatisée pour les utilisateurs.
- Workflow d'approbation pour les demandes de réinitialisation de mot de passe.

1.4 Outil de gestion des autorisations de dossier partagé Active Directory et NTFS

- Définition, modification ou révocation d'autorisations NTFS
- Ajout, modification ou suppression d'autorisations de partage
- Délégation de gestion des serveurs de fichiers Windows
- Bonnes pratiques de gestion des autorisations

ADManager Plus, solution Web de gestion et de suivi Active Directory (AD), réunit les fonctionnalités d'un outil complet de gestion des identités et d'un outil de gestion des autorisations de serveur de fichiers en une seule console. ADManager Plus permet de gérer simultanément les autorisations d'accès de plusieurs dossiers et fichiers, ou d'affecter précisément des autorisations à certains dossiers ou fichiers.

Gestion des serveurs de fichiers

Éliminez tout risque d'usage abusif ou d'altération de données avec une gestion des autorisations rigoureuse et précise. Modifiez ou supprimez facilement des autorisations NTFS et de partage en quelques clics.

1.5 Outil de gestion des groupes Active Directory

Un groupe Active Directory conçu de manière stratégique simplifie l'administration et assure une flexibilité maximale. Toutefois, configurer les groupes et définir leurs divers attributs est une procédure complexe qui implique de nombreuses étapes en cas d'exécution avec les outils natifs Active Directory, PowerShell, etc. Pour éviter ce problème et simplifier la gestion des groupes, ADManager Plus rationalise chaque tâche et vous assiste pour administrer les groupes dans une console Web centralisée.

ADManager Plus offre une fonctionnalité exclusive dédiée à la gestion des groupes qui simplifie la création et la mise à jour des groupes de sécurité et de distribution dans Active Directory. Vous pouvez ajouter/supprimer plusieurs membres de groupe, définir divers attributs, configurer des attributs Exchange et effectuer une importation en masse depuis un fichier CSV en une seule opération.

Dans ADManager Plus, la fonctionnalité de gestion des groupes Active Directory vous permet de :

- Créer des groupes Active Directory
- Modifier des groupes Active Directory
- Modifier les attributs de groupe d'utilisateurs AD
- Configurer les attributs Exchange de groupes AD

Création de plusieurs membres dans un groupe

Créer des groupes de sécurité et de distribution est une tâche simple avec ADManager Plus, qui permet d'importer tous les membres (depuis un fichier CSV) ou de les sélectionner dans une liste pour créer un groupe. Vous pouvez également définir dans la même fenêtre les propriétés Exchange des groupes. Vous disposez même de ble modèles de création de groupe personnalisables pour affiner le processus selon les politiques et les besoins de votre organisation.

Modification de plusieurs membres d'un groupe

ADManager Plus vous permet de modifier des groupes Active Directory en sélectionnant simplement le groupe et en important les membres ou en les choisissant dans une liste. Vous évitez ainsi d'avoir à sélectionner des utilisateurs individuels et à modifier leur association avec

les groupes respectifs dans Active Directory. L'étendue des groupes reste inchangée pour des questions de sécurité.

Modification des attributs de groupe d'utilisateurs

Contrairement aux outils Active Directory natifs qui permettent uniquement de modifier des attributs pour un seul membre à la fois, ADManager Plus offre une modification en masse de ces attributs de groupe. Les opérations de groupe comme l'ajout ou la suppression de membres et la définition des groupes principaux sont réalisables sur des objets Groupe dans Active directory. Vous n'avez pas à gérer individuellement les membres et pouvez les importer depuis un fichier CSV ou les choisir dans une liste.

Configuration des attributs Exchange de groupes

Vous pouvez configurer les propriétés Exchange des groupes lors de leur création ou modification. Cela vous permet de définir l'adresse électronique, l'alias de messagerie, les restrictions de remise et d'autres attributs des groupes Active Directory.

1.6 Gestion Office 365 et Exchange

ADManager Plus permet de gérer et de suivre les objets Active Directory (AD), Office 365 et Microsoft Exchange, le tout dans une seule console.

Gestion des utilisateurs

Créez des comptes Office 365 pour les utilisateurs AD, réinitialisez des mots de passe, bloquez, débloquez ou supprimez des comptes et configurez l'authentification multifacteur (MFA).

Gestion des licences

Affectez, supprimez ou remplacez en masse des licences pour des utilisateurs Office 365. Ajoutez ou supprimez des licences d'utilisateur selon les appartenances à des groupes.

Gestion des contacts

Créez, modifiez, masquez, affichez ou supprimez en masse des contacts Office 365 en important leurs détails d'un fichier CSV.

Gestion des groupes

Créez et attribuez en masse des appartenances à des groupes de sécurité, de distribution et de distribution dynamique Office 365 avec un fichier CSV.

Délégation de tâches Office 365 par OU

Déléguez des opérations Office 365 d'unités d'organisation (OU) données à certains techniciens en quelques clics.

Automatisation de la gestion et du suivi Office 365

Rendez totalement automatiques des tâches Office 365 essentielles comme la création de comptes d'utilisateur, la gestion des licences et l'annulation de l'attribution d'utilisateurs.

2 SUIVI

2.1 Rapports des utilisateurs Active Directory

La surveillance et l'analyse des modifications dans Microsoft Active Directory constituent l'une des principales difficultés auxquelles se heurte chaque administrateur informatique. Les rapports d'utilisateur de ADManager Plus fournissent un aperçu complet du domaine Windows Active Directory, qui compte de multiples unités organisationnelles et de nombreux utilisateurs, afin de surveiller et gérer les comptes d'utilisateurs de manière proactive ; le traitement de ces tâches, qui sinon s'avèreraient longues et fastidieuses, s'en trouve facilité et le processus de création de rapports est également simplifié.

Alors qu'avec les outils AD natif vous ne pouvez choisir qu'entre PowerShell ou d'autres méthodes de script pour élaborer tous les rapports dont vous avez besoin en partant de zéro, ADManager Plus offre une liste complète de rapports d'utilisateur préconfigurés Active Directory, qui permettent de créer des rapports et de gérer de manière efficace et sans tracas les comptes d'utilisateurs, et qui présentent les principaux attraits suivants :

- Interface utilisateur intuitive entièrement basée sur le Web.
- Complètement personnalisable.
- Options de Mise à jour / Modification instantanée.
- Facile à générer / Planifier les rapports / Génération automatique de rapports.
- Format de tableau simple..
- Restriction de la génération des rapports à des unités organisationnelles spécifiques.
- Exportables sous différents formats (CSV, Excel, PDF, HTML, CSVDE).
- Basé sur la conformité (SOX, HIPAA, etc.).

Les rapports d'utilisateur sont importants pour obtenir des informations vitales comme les utilisateurs ayant l'autorisation d'ouverture de session de l'utilisateur à distance, les utilisateurs dont la boîte aux lettres est activée, les utilisateurs avec OMA / OWA activé, etc.

ADManager Plus propose plus de 25 rapports planifiables sur les objets utilisateur classés dans les quatre principales catégories suivantes :

Rapports d'utilisateur généraux

Sous les Rapports d'utilisateur généraux, le rapport Tous les utilisateurs fournit des informations détaillées sur tous les utilisateurs dans le domaine sélectionné comme la création, la suppression de comptes d'utilisateurs, les informations sur les groupes, les modifications apportées aux attributs, etc. Pour rechercher les utilisateurs ayant des valeurs d'attribut vides, vous pouvez générer le rapport Utilisateurs ayant des attributs vides. L'historique des mises à jour récentes des utilisateurs peut être consulté dans le Rapport des utilisateurs créés récemment, le Rapport des utilisateurs supprimés récemment et le Rapport des utilisateurs modifiés récemment. Vous pouvez générer des rapports spécialisés pour détecter les utilisateurs ayant des scripts d'ouverture de session ainsi que les utilisateurs sans script d'ouverture de session.

Liste des rapports d'utilisateur :

- Active Directory All Users Report
- Rapport Tous les utilisateurs
- Rapport Utilisateurs ayant des attributs vides

- Rapport Utilisateurs sans gestionnaires
- Rapport Utilisateurs basés sur les gestionnaires
- Rapport Utilisateurs présents dans plus d'un groupe
- Rapport Utilisateurs supprimés récemment
- Rapport Utilisateurs créés récemment
- Rapport Utilisateurs modifiés récemment
- Rapport Autoriser l'accès aux appels entrants
- Rapport Refuser l'accès aux appels entrants
- Rapport Utilisateurs avec script d'ouverture de session
- Utilisateurs activés Lync
- Utilisateurs activés Lync
- Utilisateurs désactivés Lync
- Rapports des statuts des comptes d'utilisateurs

De même, dans la catégorie des rapports des statuts des comptes d'utilisateurs figurent des rapports spécialisés où sont extraits les détails des utilisateurs désactivés et des utilisateurs verrouillés ainsi que des informations sur les dates d'expiration des comptes d'utilisateurs. Les Rapports des utilisateurs dont le compte a expiré, des utilisateurs dont le compte a expiré récemment, des comptes d'utilisateurs qui vont expirer bientôt, et des utilisateurs dont les comptes n'expireront jamais peuvent être conservés dans cet ensemble de rapports d'utilisateurs Active Directory, ce qui facilitera l'administration et la gestion des comptes d'utilisateurs.

Liste des rapports des statuts des comptes :

- Active Directory Disabled Users Report
- Rapport Utilisateurs désactivés
- Rapport Utilisateurs verrouillés
- Rapport Utilisateurs dont le compte a expiré
- Rapport Utilisateurs dont le compte a expiré récemment
- Rapport Utilisateurs dont le compte expirera bientôt
- Rapport Utilisateurs dont le compte n'expire jamais
- Rapports d'ouverture de session d'utilisateur

Dans les Rapports d'ouverture de session d'utilisateur figure l'historique des informations de connexion de l'utilisateur. Il est possible de planifier la génération des rapports sur les utilisateurs inactifs (les utilisateurs qui n'ont pas ouvert de session pendant une certaine période), les utilisateurs qui ont ouvert une session récemment, les utilisateurs qui n'ont jamais ouvert de session et les utilisateurs activés. Le rapport basé sur les heures d'ouverture de session vous donnera une idée précise des utilisateurs qui ont ouvert une session pendant un intervalle de temps spécifié.

Liste des rapports d'ouverture de session d'utilisateur :

- Active Directory Inactive Users Reports
- Rapport Utilisateurs inactifs
- Rapport Utilisateurs qui ont ouvert une session récemment
- Rapport Heures réelles de la dernière ouverture de session d'utilisateur
- Rapport basé sur l'heure d'ouverture de session
- Rapport Utilisateurs n'ayant jamais ouvert de session
- Rapport Utilisateurs activés
- Rapport Utilisateurs activés

Les informations sur le groupe de l'utilisateur peuvent être décodées avec le rapport des utilisateurs imbriqués. Ces rapports permettent de comprendre les détails relatifs aux utilisateurs dans un groupe particulier et les détails des multiples groupes auxquels un utilisateur appartient.

Liste des rapports des utilisateurs imbriqués :

- Active Directory Users in a Group Report
- Rapport Utilisateurs dans un groupe
- Rapport Groupes pour un utilisateur
- Rapports d'utilisateurs Active Directory pour les audits de conformité SOX

ADManager Plus peut être un outil efficace pour vous aider à respecter les exigences d'audit de conformité. Un ensemble complet de rapports indispensables peuvent être générés et utilisés comme ressource clé pour répondre aux audits de conformité.

2.2 Rapports sur la connexion des utilisateurs Active Directory

Les rapports sur la connexion des utilisateurs fournissent facilement des détails sur la connexion d'un compte d'utilisateur Active Directory, comme la date et l'heure auxquelles un utilisateur se connecte à un réseau Windows. Ces informations sont cruciales pour les administrateurs réseau afin de suivre l'activité des utilisateurs dans l'environnement Active Directory et déterminer ceux qui ne sont pas connectés pendant une certaine période, lister toutes les connexions d'utilisateur à distance, contrôler la date de la dernière connexion réelle des utilisateurs, le temps de connexion, etc. Ils peuvent ainsi effectuer des tâches comme la suppression ou le nettoyage des utilisateurs inactifs ou désactivés, modifier les temps de connexion autorisés et autres en masse. Les outils natifs de Microsoft Windows Active Directory, PowerShell, etc. ne procurent pas de données sur la dernière connexion réelle de plusieurs domaines, car l'un des contrôleurs de domaine peut authentifier la connexion de l'utilisateur sans que la réplication des données de connexion ne se produise entre eux.

ADManager Plus offre une solution qui facilite le suivi en permettant aux administrateurs Active Directory de surveiller l'activité de connexion et de déconnexion des utilisateurs via ses rapports sur la connexion des utilisateurs Active Directory. Les données de connexion extraites sont synchronisées et obtenues en contactant différents contrôleurs de domaine et serveurs simultanément. Ces rapports contiennent des détails relatifs à la connexion/déconnexion des utilisateurs comme les utilisateurs non connectés au cours des n derniers jours, les dernières connexions au contrôleur de domaine, les dates des dernières connexions réelles, etc.

ADManager Plus offre les rapports suivants sur la connexion au réseau :

- Rapport sur les utilisateurs inactifs
- Rapport sur les utilisateurs connectés récemment
- Rapport sur les utilisateurs jamais connectés
- Rapport sur la dernière date de connexion réelle des utilisateurs
- Rapport sur les utilisateurs basé sur les heures de connexion
- Rapport sur les utilisateurs à connexion activée

Ces rapports sur la dernière connexion Windows 2000/2003, dont vous pouvez automatiser la génération et l'exportation, améliorent la gestion en extrayant des données de connexion

exactes pour les utilisateurs depuis la configuration Active Directory de l'organisation. Comme ADManager Plus est un outil Web, il permet une gestion et un suivi Active Directory à distance. Grâce au téléchargement gratuit d'une version d'évaluation de la solution valable 30 jours, découvrez en détail comment ces rapports améliorent la gestion des comptes d'utilisateurs.

Rapport sur les utilisateurs inactifs

Il faut identifier les utilisateurs Active Directory inactifs pendant une période donnée de manière régulière. La liste des utilisateurs AD inactifs repose sur la dernière date de connexion des utilisateurs. Tous les contrôleurs de domaine configurés sont analysés pour déterminer cette date afin de garantir l'exactitude des données.

Rapport sur les utilisateurs connectés récemment (date de connexion des utilisateurs)

Ce rapport fournit des détails sur tous les utilisateurs Active Directory qui se sont connectés au cours des n derniers jours. Les utilisateurs AD connectés récemment sont déterminés d'après leur dernière date de connexion. Tous les contrôleurs de domaine configurés sont analysés pour déterminer cette date afin de garantir l'exactitude des données.

Rapport sur les utilisateurs jamais connectés

Ce rapport affiche la liste des utilisateurs qui ne se sont pas connectés une seule fois au domaine. La dernière date de connexion n'est mise à jour dans le domaine que si l'utilisateur se connecte au moins une fois. Ce rapport repose sur cette caractéristique d'Active Directory.

Rapport sur les utilisateurs basé sur les heures de connexion

Ce rapport fournit des données complètes sur les heures de connexion autorisées de l'utilisateur Active Directory. ADManager Plus vous permet de générer des rapports sur les heures de connexion autorisées et refusées pour les jours sélectionnés et la date indiquée.

Rapport sur la dernière date de connexion réelle

Ce rapport liste les dernières dates de connexion réelles des utilisateurs. En d'autres termes, il affiche la date et l'heure réelles auxquelles les utilisateurs se sont connectés pour la dernière fois au réseau. Les détails sont extraits en interrogeant tous les contrôleurs de domaine configurés pour garantir l'exactitude des données.

Rapport sur les utilisateurs à connexion activée

Ce rapport génère une liste de tous les utilisateurs Active Directory actifs. Il affiche des détails sur tous les utilisateurs AD qui se connectent au réseau régulièrement. Il est complémentaire du rapport sur les utilisateurs inactifs.

En outre, cet outil simplifie la gestion Active Directory grâce à sa fonction d'exécution d'actions à partir des rapports. Vous pouvez ainsi effectuer des tâches de gestion des utilisateurs comme l'activation, la désactivation, le déverrouillage ou la suppression de comptes directement depuis les rapports. ADManager Plus fonctionne comme un outil de gestion et de suivi Active Directory automatique efficace. Point capital : vous réalisez toutes ces opérations en quelques clics seulement, sans aucune ligne de script.

2.3 Rapports sur les autorisations NTFS pour Active Directory :

- Rapport sur les autorisations de contrôle d'accès des utilisateurs et des groupes
- Liste des autorisations de dossier
- Exportation d'autorisations de dossier vers Excel
- Prévention d'un accès non autorisé aux partitions NTFS
- Automatisation du suivi des autorisations

Analysez et affinez les autorisations de partage et les listes ACL avec notre outil de suivi ADManager Plus, solution de gestion et de suivi Active Directory, offre un outil de suivi des autorisations de dossier partagé pour les serveurs Isilon et NetApp. Elle propose des rapports prédéfinis pour afficher, analyser et modifier les autorisations NTFS et de partage ou les listes de contrôle d'accès (ACL) affectées à des serveurs, des dossiers et des fichiers Windows ou NetApp.

ADManager Plus permet de :

1/ Suivre les autorisations de contrôle d'accès des utilisateurs et des groupes Active Directory
Rapport sur les autorisations de dossier : examinez les utilisateurs et les groupes ayant accès à des dossiers sur un chemin donné. Les entrées de contrôle d'accès associées indiquent le niveau d'accès d'un utilisateur ou groupe sur un dossier et définissent les autorisations transmissibles, le cas échéant.

Comment afficher les utilisateurs et les groupes ayant accès à un dossier précis avec ADManager Plus :

Connectez-vous à ADManager Plus et accédez au rapport Autorisations de dossier.

Indiquez le chemin du dossier et le niveau d'accès.

Générez le rapport.

Rapports de sécurité : affichez une liste de tous les serveurs, sous-réseaux ou objets accessibles par un compte d'utilisateur donné.

Permissions for Folders reportSecurity reports

2/ Afficher les autorisations de dossier

Rapport sur les partages de serveur : affichez tous les partages disponibles sur les serveurs indiqués, avec des détails importants comme leur emplacement, la liste des comptes ayant des autorisations sur les partages (principaux de sécurité), les autorisations afférentes et leur étendue (par exemple, dossier ou sous-dossier).

Rapport des dossiers accessibles par des comptes : filtrez tous les dossiers et les fichiers selon leurs autorisations de compte particulières. Vérifiez les dossiers sur un chemin donné et définissez mieux le niveau d'accès (contrôle total ou autre) pour obtenir une liste de résultats.

Rapport sur les dossiers non transmissibles : affichez les dossiers et les fichiers ne pouvant pas hériter d'autorisations. Indiquez le chemin pour obtenir une liste de tous les fichiers et les dossiers qui ne peuvent pas hériter des autorisations de leurs objets parents.

Shares in the Servers reportFolders Accessible by Accounts reportNon-inheritable Folders report

3/ Exporter des autorisations de dossier au format Excel ou autre
Exportez les autorisations NTFS et de partage de fichiers et de dossiers au format Excel ou CSV, HTML, PDF et CSVDE.

4/ Empêcher un accès non autorisé aux partitions et partages NTFS
Assurez un suivi complet des autorisations NTFS et de partage de tous les fichiers et les dossiers pour éviter un usage abusif de fichiers, notamment l'altération du contenu du fait d'un accès non autorisé. Générez des rapports sur les autorisations d'accès pour des fichiers, dossiers et partages de serveur. Descendez jusqu'au dossier ou fichier réel et analysez les paramètres de sécurité et les ACL pour pouvoir prendre des mesures adéquates et normaliser le contrôle d'accès utilisateur.

5/ Automatiser le suivi des autorisations NTFS et de partage
Planifiez la génération des rapports au moment voulu. Une fois générés, ces rapports peuvent être automatiquement envoyés à l'administrateur.

Avantages d'utiliser ADManager Plus comme outil de suivi des autorisations NTFS :
Génération de rapports détaillés sur les autorisations NTFS, les partages et les ACL sans script PowerShell.
Planification et exportation de rapports au format CSV, PDF, HTML ou CSVDE.
Exécution d'opérations de gestion des autorisations de serveur de fichiers dans une console.

2.4 Rapports de groupes Active Directory

Les rapports de groupes Active Directory permettent aux administrateurs d'obtenir une vue rapide des groupes de sécurité, des groupes de distribution, des principaux grands groupes en termes d'objets, etc., en quelques clics. Ces rapports vous libèrent de la tâche fastidieuse d'écrire des scripts pour la création de rapports Active Directory. Grâce aux rapports planifiables basés sur l'interface graphique de cet outil, la création de rapports Active Directory est simplifiée. En outre, cet outil simplifie même la gestion Active Directory grâce à sa fonctionnalité permettant d'effectuer des actions de gestion directement à partir des rapports.

Contrairement aux outils Exchange natifs, PowerShell, etc., ADManager Plus fournit les rapports basés sur les groupes prêts à l'emploi suivants, notamment les groupes créés, modifiés ou supprimés récemment, que vous pouvez générer et exporter automatiquement ou chaque fois que vous en avez besoin :

Groupes de sécurité

Fournit les détails des groupes de sécurité disponibles dans les domaines sélectionnés. Un groupe de sécurité est utilisé pour regrouper des utilisateurs, des ordinateurs et d'autres groupes afin d'affecter des autorisations aux ressources.

Groupes de distribution

Fournit les détails des groupes de distribution disponibles dans les domaines sélectionnés. Les groupes de distribution sont utilisés pour créer des listes de distribution de courrier électronique.

Types et étendues des groupes

Fournit les détails des groupes en fonction du type et de l'étendue des groupes. En d'autres termes, il fournit des détails sur le type de groupe, par exemple s'il s'agit d'un groupe de sécurité ou de distribution, ainsi que des informations sur l'étendue du groupe, comme Global, Domaine local ou Universel. Cet outil offre également des rapports pour suivre les groupes qui sont créés, modifiés ou supprimés à partir d'Active Directory.

Groupes sans membres

Rapport pour obtenir la liste des groupes dans les domaines qui n'ont aucun membre. Il permet aux administrateurs d'identifier les groupes qui sont vides et qui ne sont plus utilisés.

Membres de groupes détaillés

Rapport pour récupérer la liste complète de tous les objets qui sont membres du groupe Active Directory spécifié ainsi que de ses groupes imbriqués. Voici les points forts de ce rapport :

Récupère les informations sur tous les membres - utilisateurs, groupes, ordinateurs et contacts - de tout groupe Active Directory, y compris ses groupes imbriqués.

Possède des filtres puissants qui vous permettent de :

- Sélectionner uniquement les objets Active Directory requis.
- Inclure/exclure des attributs spécifiques ou choisir uniquement les attributs dont vous avez besoin dans les rapports, pour tous les objets sélectionnés.

Possibilité de visualiser les données extraites dans un format de tableau ou sous forme de résumé par objet qui peut être exploré au niveau du détail pour afficher des détails spécifiques.

N premiers grands groupes

Rapport pour déterminer quels sont les grands groupes dans le domaine en fonction du nombre d'objets qu'ils contiennent.

Groupes avec gestionnaires

Rapport pour afficher les groupes avec gestionnaires. Un gestionnaire de groupe aura le contrôle complet sur les utilisateurs de ce groupe.

Groupes sans gestionnaires

Rapport pour afficher les groupes sans gestionnaires.

Utilisateurs ne faisant pas partie de groupes

Si l'administrateur souhaite faire le point sur les appartenances des utilisateurs à des groupes, ce rapport identifiera les utilisateurs qui ne sont pas membres du ou des groupes sélectionnés.

Groupes imbriqués

Rapport pour identifier les groupes dont un utilisateur spécifique est membre. Il ne répertorie que les utilisateurs dans des groupes imbriqués. Par exemple, l'utilisateur John est membre du groupe Utilisateurs, qui est lui-même membre du groupe Utilisateurs du domaine. Par conséquent, John est également membre du groupe Utilisateurs du domaine.

Outre les rapports de groupe préconstruits, cet outil fournit également des rapports d'utilisateurs, des rapports d'ordinateurs, des rapports d'objets de stratégie de groupe (GPO), etc. pour une création de rapports Active Directory simplifiée et rapide. De plus, avec ses

rapports spécifiques au serveur Exchange Server, cet outil facilite également la création de rapports Exchange.

2.5 Réponse aux exigences de conformité avec les rapports d'ADManager Plus

Les organisations modernes doivent non seulement s'efforcer de protéger les données contre les cybermenaces actuelles, mais aussi de veiller à se mettre en conformité avec les réglementations courantes en la matière. Avec l'avènement des réglementations de conformité comme SOX, HIPAA, PCI DSS, GLBA et RGPD, les organisations ont subi de profonds changements ces dernières années. Les organisations ne peuvent plus tenir des registres financiers sommaires simplement pour répondre à un audit rapide ponctuel. La conformité oblige à présent à consigner avec précision les activités courantes et à conserver des archives pour les périodes que recommandent ces nouvelles réglementations.

Les directives de ces réglementations de conformité semblent viser à éviter tout risque de manipulation des données et, dans le cas des normes SOX, PCI et GLBA, à n'omettre aucun élément constituant l'information financière. Bien que ces exigences améliorent la sécurité, la mise en conformité avec celles-ci s'avère difficile du fait de leur grande complexité. La majorité des données liées à ces réglementations relèvent de tâches organisationnelles ayant lieu dans Active Directory (AD), mais nombre d'organisations manquent d'un système de suivi complet pour l'activité AD. Il devient quasiment impossible à présent de remplir les exigences de conformité sans l'aide d'une solution dédiée.

ADManager Plus, notre solution de gestion et de suivi AD, offre un système de suivi global qui couvre divers aspects de la gestion de la conformité. Il accède au cœur de Windows et d'Active Directory pour obtenir les données qu'exige un audit de conformité et permet de les exporter. De plus, contrairement aux outils AD natifs (comme PowerShell) qui restent lourds et chronophages à utiliser, ADManager Plus présente ces données dans un format convivial avec de nombreux filtres pour n'afficher que les détails requis. On peut facilement extraire et exporter les informations nécessaires pour remplir les exigences de conformité réglementaire comme HIPAA, PCI DSS, GLBA, SOX et GDPR.

Conformité HIPAA

La norme HIPAA (Health Insurance Portability and Accountability Act, ou loi américaine sur la portabilité et la responsabilité des assurances maladie) vise à protéger les données sensibles des patients. ADManager Plus offre des rapports prédéfinis d'audit AD pour assurer la conformité avec cette norme.

Conformité PCI-DSS

Toute entreprise traitant des données de carte de paiement doit respecter la norme PCI-DSS (Payment Card Industry Data Security Standard, ou norme de sécurité des données du secteur des cartes de paiement). ADManager Plus offre une série de rapports interactifs qui aident l'organisation à gérer les aspects de l'environnement AD concernant ces exigences réglementaires.

Conformité GLBA

La loi Gramm-Leach-Bliley Act (GLBA) oblige les organisations à prendre des mesures pour protéger les données sensibles et à expliquer leurs pratiques de diffusion d'informations à leurs

clients. Les rapports complets d'ADManager Plus permettent de répondre à des questions cruciales sur la conformité GLBA.

Conformité SOX

La loi Sarbanes-Oxley (SOX) vise à renforcer les procédures et les exigences en matière d'audit et de suivi financier pour réduire le risque de fraude des entreprises. ADManager Plus offre des rapports prêts à l'emploi pour vérifier la protection des ressources contre un accès illicite. En savoir plus

Conformité RGPD

Si l'organisation traite des données de citoyens résidant dans l'Union européenne, le Règlement général sur la protection des données (RGPD) l'oblige alors à prendre des mesures pour éviter tout accès non autorisé aux informations sur les clients. ADManager Plus offre des rapports d'audit AD prêts à l'emploi pour la mise en conformité RGPD.

2.6 Rapports sur les licences Office 365

ADManager Plus donne un aperçu détaillé des aspects vitaux de l'infrastructure Office 365 avec une gamme de rapports prédéfinis. Ses rapports sur les licences Office 365 extraient les détails clés des licences Office 365 attribuées à divers utilisateurs de l'organisation, sans besoin de script PowerShell complexe.

Le détail des licences Office 365 est essentiel pour les administrateurs afin d'assurer une utilisation optimale des licences et des services dans l'organisation. Ils peuvent déterminer les licences valides et disponibles et les réaffecter en conséquence aux bons utilisateurs. Cela permet aux administrateurs de maîtriser le coût des licences en évitant un achat inutile ou imprévu d'autres licences. On peut aussi exporter le résultat de rapports au format PDF, CSV, XLSX ou HTML selon le besoin.

Les rapports sur les licences Office 365 d'ADManager Plus comprennent :

- Rapport sur les utilisateurs sous licence

Affichez les détails de tous les utilisateurs de l'environnement Office 365 disposant de licences, avec la liste des services disponibles via chaque licence. L'information que fournit ce rapport permet de décider si les licences et les services nécessaires ont été attribués aux utilisateurs et d'effectuer les modifications voulues pour utiliser efficacement les licences acquises.

- Rapport sur les utilisateurs sans licence

Affichez les détails de tous les utilisateurs de l'environnement Office 365 ne disposant pas de licences. Cette information permet d'identifier les utilisateurs de l'organisation ayant besoin de licences, pour mieux prévoir l'acquisition de nouvelles licences de façon calculée et précise.

- Rapport sur les détails des licences

Affiche toutes les licences déployées dans l'environnement Office 365. Pour chaque licence, le rapport énumère les unités actives, affectées, avec des avertissements, suspendues et verrouillées. L'étude de cette information aide à déterminer les licences inutilisées afin de les attribuer à des utilisateurs en ayant besoin. Elle permet aussi d'évaluer la demande et l'offre de licences dans l'organisation et de les comparer à l'utilisation.

ADManager Plus offre non seulement des rapports sur les licences Office 365 de façon simple et sans script, mais aussi une gamme d'autres rapports, outre les fonctionnalités prêtes à l'emploi qui facilitent la gestion des comptes Office 365. Outre Office 365, la solution permet de gérer efficacement plusieurs domaines Active Directory ou un environnement Exchange, dans une console unique.

Autres fonctionnalités

Rapports sur les utilisateurs Office 365

Générez des rapports détaillés sur les utilisateurs Office 365 avec les rapports prêts à l'emploi qu'offre ADManager Plus. On peut planifier des rapports pour une exécution régulière.

Gestion Office 365

Gérez les utilisateurs, les licences, les contacts, les groupes et d'autres objets Office 365 avec de simples actions par pointer-cliquer. Rendez la gestion Office 365 facile comme un jeu d'enfant !

Automatisation Office 365

Choisissez parmi des actions prédéfinies et automatisez les opérations les plus courantes, comme l'attribution d'utilisateurs, la gestion des licences ou la gestion des photos, sans script.

Gestion des licences Office 365

Ajoutez, remplacez et supprimez instantanément des licences Office 365 pour assurer une gestion optimale dans toute l'organisation grâce à ADManager Plus.

Gestion des boîtes aux lettres partagées Office 365

Créez et modifiez en masse des boîtes aux lettres partagées Office 365 et déléguez leur gestion sans script PowerShell. La gestion des boîtes aux lettres partagées n'a jamais été aussi facile !

Rapports sur les groupes Office 365

Un catalogue complet contient chaque rapport sur les groupes Office 365 dont on peut avoir besoin, de façon intégrée à la solution ! On peut planifier des rapports pour une exécution régulière.

3 Automatisation

3.1 Création/attribution d'utilisateurs Active Directory automatisée

Lorsqu'on envisage l'automatisation Active Directory, le premier point venant à l'esprit concerne la capacité d'automatiser la création/attribution d'utilisateurs sans lacunes. Les outils comme PowerShell ou des scripts ne faisant qu'aggraver la complexité, il importe de choisir une bonne solution d'automatisation Active Directory qui offre un système d'attribution d'utilisateurs bien planifié et normalisé. Elle doit allier complétude fonctionnelle et rentabilité.

Conciliant au mieux ces deux exigences, ADManager Plus offre l'une des solutions les plus fiables sur le marché pour automatiser la gestion Active Directory. Pour vous en convaincre, examinons plus en détail la solution et ses fonctionnalités.

Une fonction pour résoudre chaque problème lié à une attribution d'utilisateurs automatisée
L'attribution d'utilisateurs automatisée ne se résume pas à un fichier de commandes exécuté à une heure prévue, produisant des centaines ou des milliers de comptes d'utilisateur. Elle va au-delà. Examinez le tableau suivant pour en savoir plus.

Caractéristiques de l'attribution d'utilisateurs automatisée avec ADManager Plus

Système de workflow d'approbation

Définition

Un système de workflow d'approbation permet de créer une hiérarchie linéaire d'approbation de processus pour l'automatisation. Cela consiste à indiquer ceux qui configurent et lancent le processus automatisé, qui l'examinent et qui l'approuvent.

En d'autres termes, on peut ainsi intégrer des jalons de supervision à des points cruciaux du processus automatisé.

Raison de son importance

L'automatisation de l'attribution d'utilisateurs revêt un rôle clé et il ne faut donc pas la négliger. De plus, plusieurs exigences réglementaires imposent un système de supervision pour suivre et documenter toutes les tâches cruciales comme l'attribution d'utilisateurs et la désactivation.

Format de dénomination avancée d'identification unique

Définition

Ce format de dénomination permet de marquer des noms et des adresses électroniques avec un identifiant unique (que vous indiquez) afin d'éviter la duplication.

Raison de son importance

Un processus d'attribution d'utilisateurs en masse présente souvent un problème de noms en double. ADManager Plus évite aisément ce problème grâce à son format de dénomination avancée.

Format de dénomination réactive

Définition

Il s'agit d'un widget dont le rôle consiste à désigner les comptes d'utilisateur et leurs propriétés. On peut le configurer pour improviser des noms avec les données fournies.

Raison de son importance

L'une des raisons les plus courantes d'échecs répétés de la création/attribution d'utilisateurs réside dans un fichier CSV ayant des champs manquants.

Modèle d'attribution de comptes d'utilisateur

Définition

Il s'agit de l'aspect le plus important de tous ! ADManager Plus permet de normaliser l'attribution d'utilisateurs. On peut enregistrer toutes les configurations des propriétés de compte d'utilisateur et des boîtes aux lettres dans un modèle et l'appliquer aux comptes lorsqu'on en crée !

Raison de son importance

L'attribution d'utilisateurs étant lourde et chronophage, un moyen de l'accélérer et la faciliter comme celui-ci s'avère des plus utiles. De plus, on peut définir chaque configuration requise pour un compte d'utilisateur dans une seule fenêtre !

Automatisation de l'attribution d'utilisateurs avec ADManager Plus En arrière-plan

Dans ADManager Plus, il suffit de procéder ainsi pour automatiser l'attribution d'utilisateurs :

- Définissez la date d'exécution du processus.
- Indiquez le chemin d'accès du fichier CSV.
- Choisissez un modèle de création d'utilisateur à appliquer.
- Selon le besoin, décidez de déployer ou non le workflow.

Le processus démarre alors chaque fois que la fonction d'automatisation découvre un fichier CSV nouveau ou mis à jour dans son exécution planifiée. Elle effectue la création et avertit simplement les concernés ou, en cas d'automatisation contrôlée (déploiement d'un workflow opérationnel), elle produit un rapport clair des comptes d'utilisateur à créer et attend que le réviseur (défini dans le workflow utilisé) examine la demande et décide de l'approuver pour la traiter.

Dans ADManager Plus, l'attribution d'utilisateurs automatisée s'avère si simple et fiable (car il est toujours possible de lancer le processus via le workflow pour veiller à vérifier la tâche à chaque phase) que l'on peut déléguer cette tâche même à un non-technicien du service RH.

Stratégie d'automatisation

ADManager Plus permet d'automatiser toutes les tâches de suivi pour l'attribution d'utilisateurs. Par exemple, supposons que vous adoptez l'automatisation pour créer des comptes d'utilisateur pour des étudiants admis à un cours de deux mois en mars. La stratégie d'automatisation permet aussi de définir le processus pour supprimer automatiquement les comptes après une période de deux mois (plusieurs tâches de suivi sont configurables).

Principaux avantages de l'utilisation d'ADManager Plus pour l'attribution automatisée des utilisateurs AD :

- Automatisation de l'ensemble du processus de création d'utilisateurs AD pour gagner du temps et de l'énergie.
- Automatisation de l'attribution des utilisateurs AD basée sur l'examen et l'approbation.
- Suivi de l'ensemble du processus d'automatisation via des rapports

3.2 Nettoyer votre Active Directory

Au fil du temps, les comptes d'utilisateur et d'ordinateur deviennent obsolètes et doivent être éliminés. ADManager Plus vous aide à localiser tous les utilisateurs et les ordinateurs inactifs, désactivés ou dont les comptes ont expiré dans Active Directory. En fonction de la stratégie de gestion interne d'Active Directory définie par votre entreprise, vous pouvez éliminer tous les comptes inutiles en les supprimant, ou nettoyer effectivement et efficacement votre Active Directory avec les fonctions désactiver, activer ou déplacer des comptes.

Vous améliorerez ainsi la sécurité et la performance de votre Active Directory, et vous pourrez gagner un temps considérable en évitant de devoir utiliser des outils et des scripts de ligne de commande.

Fonctionnalités

- Trouver les comptes d'utilisateur ou d'ordinateur qui ne se sont pas connectés depuis un nombre X de jours
- Trouver les comptes Active Directory expirés et inutilisés
- Désactiver, déplacer, supprimer des comptes d'utilisateur ou d'ordinateur et désactiver, supprimer, déplacer ou activer des comptes Active Directory en quelques secondes.
- Affiche les comptes désactivés, l'heure de la dernière ouverture de session/fermeture de session, le type de système d'exploitation, etc.
- Exporter des rapports aux formats CSV, XLS, HTML, PDF et CSVDE.

Recherche de comptes périmés sur votre réseau

Les rapports suivants d'ADManager Plus vous aideront à détecter et supprimer les comptes dormants dans votre Active Directory :

- Générer une liste de comptes désactivés
- Générer une liste de comptes inactifs
- Générer une liste d'utilisateurs dont les comptes ont expiré
- Gérer les comptes dormants ou périmés : Les supprimer, les désactiver ou les déplacer vers une autre unité d'organisation.

Comptes désactivés

Avec ADManager Plus vous pouvez facilement générer la liste des comptes d'utilisateur ou d'ordinateur qui sont désactivés pour une raison ou une autre. L'attribut userAccountControl est utilisé pour identifier les utilisateurs désactivés dans le domaine. Vous pouvez facilement gérer ces comptes en les supprimant ou en les déplaçant vers une autre unité d'organisation. Vous pouvez aussi supprimer/activer/déplacer deux ou plusieurs comptes désactivés en même temps.

Utilisateurs dont le compte a expiré

Les comptes d'utilisateur Active Directory qui sont devenus obsolètes depuis longtemps peuvent avoir expiré sans que l'utilisateur ou l'administrateur en soit informé. Parce qu'il peut s'avérer fastidieux d'écrire un script pour trouver les comptes expirés, le générateur de rapports ADManager Plus analyse Active Directory et vous donne une liste de tous les comptes expirés. Depuis la page de résultats, vous pouvez sécuriser le réseau de façon proactive en supprimant, désactivant ou déplaçant les utilisateurs expirés vers une unité d'organisation moins privilégiée.

Vous avez aussi la possibilité d'imprimer ou d'exporter les données de résultats des utilisateurs verrouillés aux formats XLS, CSV, PDF, HTML, etc.

Utilisateurs inactifs

À l'aide d'ADManager Plus, vous pouvez récupérer les comptes d'utilisateur inactifs qui ne se sont pas connectés au domaine depuis 30 ou 60 jours ou plus.

Déplacer, désactiver ou supprimer des comptes d'utilisateur ou d'ordinateur dormants ou périmés

Une infrastructure Active Directory fiable doit toujours garantir que les comptes existants sont activés et que les comptes obsolètes sont désactivés ou supprimés, afin d'assurer une productivité et une sécurité optimales. Le statut des comptes d'utilisateur Active Directory est très hypothétique, car il dépend de nombreuses stratégies de mot de passe et d'autres limitations ; dans une petite entreprise, l'administrateur peut vérifier manuellement le statut des comptes et le modifier ultérieurement, mais dans les entreprises moyennes et grandes, il est préférable d'utiliser un outil capable de déterminer le statut des comptes d'utilisateur et d'ordinateur pour ensuite les supprimer, les désactiver ou les déplacer.

ADManager Plus et ses fonctionnalités prédéfinies Supprimer, Désactiver et Déplacer aident l'administrateur à tenir à jour le statut des comptes Active Directory. Nettoyez votre Active Directory en supprimant les comptes ou gérez un ou plusieurs comptes avec la fonctionnalité Désactiver ou Déplacer en la sélectionnant dans l'un des Rapports d'utilisateur ou d'ordinateur.

3.3 Fixation de durées limitées pour l'appartenance à des groupes

ADManager Plus permet une automatisation partielle de la gestion des groupes Active Directory. On peut complètement automatiser des tâches comme la suppression ou le déplacement de groupes. ADManager Plus permet aussi d'établir une supervision de ces tâches par des délégués concernés en déployant un workflow pour l'automatisation lorsque le scénario l'exige. Hélas, les outils AD natifs ou PowerShell offrent très peu de moyens d'automatisation.

Fonctionnement de l'automatisation

Dans ADManager Plus, l'automatisation est très simple à configurer : il suffit de choisir le type de tâche à automatiser et le moment ou l'intervalle auquel exécuter la tâche. ADManager Plus traite régulièrement l'automatisation aux intervalles définis. Par exemple, supposons qu'il faut lancer une automatisation à la fin de chaque mois pour supprimer tous les groupes sans membres. Voici comment se présenterait le modèle d'automatisation.

Contrairement à l'automatisation classique sans contrôle, ADManager Plus permet de définir un workflow d'approbation, qui régit le flux du processus d'automatisation. On conserve ainsi un contrôle constant de l'automatisation, avec même la capacité de l'arrêter si nécessaire. En résumé, cette automatisation Active Directory pour la suppression ou le déplacement de groupes est un planificateur qui :

- S'exécute à un moment donné.
- Génère un rapport des groupes pour lesquels effectuer une action précise (suppression/déplacement).
- Et, en cas de besoin, qui :

S'interrompt aux arrêts définis dans le workflow.

Procède à l'exécution de la tâche une fois validée par l'examineur.

Définition d'un workflow d'approbation

Un workflow d'approbation est une hiérarchie linéaire définissant clairement les individus qui examinent et approuvent le processus. ADManager Plus offre un workflow configurable, qui permet de définir divers niveaux d'arrêts pour le processus automatisé. Pour en savoir plus sur le workflow ADManager Plus.

Facteurs X de l'automatisation pour la suppression ou le déplacement de groupe

Les facteurs X consistent en des critères de sélection. L'ensemble de critères disponible permet de créer un processus automatisé qui recherche un type de groupe particulier et effectue une action sur celui-ci. Exemple : on peut créer un processus automatisé de suppression de groupe qui ne choisit que les groupes sans membres.

Fichiers CSV

ADManager Plus permet aussi de choisir les groupes pour lesquels effectuer des opérations AD via des fichiers CSV. On peut les ajouter à un fichier CSV et configurer l'automatisation en indiquant le chemin du fichier comme emplacement.

4 Délégestion

4.1 Modèle de délégation de gestion non invasive

ADManager Plus présente un modèle de délégation exclusif à la fois facile à utiliser et fiable. Grâce à ses fonctions de gestion et de délégation de pouvoirs, l'administrateur peut autoriser des utilisateurs autres que les administrateurs comme les techniciens d'assistance, les employés des ressources humaines ou les agents de service client à effectuer certaines tâches ne nécessitant pas l'intervention d'un administrateur. Cela réduit grandement la charge de travail de l'administrateur tout en économisant beaucoup de temps et de ressources. En bref, ADManager Plus est l'outil idéal de tout administrateur en matière de délégation de tâches.

On peut penser que les techniciens d'assistance ou les employés des ressources humaines reçoivent des droits qui nuisent à la sécurité Active Directory. Aucun souci ! ADManager Plus veille à ce que l'administrateur ne cède pas la maîtrise de la gestion Active Directory, quels que soient les droits délégués à d'autres utilisateurs. D'autre part, la solution veille à ce que l'équipe d'assistance ne puisse effectuer que les tâches déléguées par l'administrateur, sans faire appel à des options complexes comme des scripts PowerShell. Elle garantit ainsi que seul l'administrateur exerce un contrôle ultime sur Active Directory, à tous les niveaux. Toutefois, ADManager Plus se démarque des autres outils de gestion Active Directory par sa capacité à déléguer des droits à des techniciens d'assistance de façon non invasive, ce qu'apprécient la plupart des administrateurs.

Modèle de délégation d'ADManager Plus :

Ce modèle de délégation non invasive assure une parfaite protection d'Active Directory, atout clé d'ADManager Plus pour offrir une sécurité de pointe des services d'annuaire. Il permet de ne pas élever les droits d'un technicien d'assistance dans Active Directory en limitant bien le rôle qu'il doit remplir. Cela signifie aussi qu'ADManager Plus contourne Active Directory pour apporter les changements qu'effectue un technicien.

Principaux aspects d'ADManager Plus :

- Le rôle de technicien est défini dans la solution et pas directement dans Active Directory, ce qui évite d'élever les droits établis.
- Aucun privilège n'est accordé au technicien dans Active Directory, il peut y apporter des changements avec la solution au nom de l'administrateur.
- La solution ne permet de créer le rôle de technicien d'assistance qu'à partir de la liste des utilisateurs figurant déjà dans Active Directory. Ce point renforce la sécurité d'Active Directory en interdisant la création directe d'un utilisateur-technicien d'assistance avec la solution.
- Le technicien ne peut pas effectuer d'autre tâche que celles qui lui sont déléguées comme défini dans le modèle. En fait, les autres onglets ne s'affichent même pas lorsque le technicien se connecte.

Toutes ces mesures garantissent que l'annuaire Active Directory reste intact, ce qui assure la sécurité.

Délégation basée sur les groupes : outre la délégation de rôles de gestion à certains utilisateurs AD, on peut aussi les déléguer à des groupes AD. Déléguer un rôle à un groupe AD aboutit à accorder des autorisations à tous les membres du groupe pour effectuer les tâches attribuées à ce rôle.

Audit des actions de gestion:

Des droits vitaux étant délégués aux équipes d'assistance ou des ressources humaines, il importe de tenir un registre exact des activités de chaque rôle délégué, exigence que remplit parfaitement une fonction appelée journaux d'audit de technicien. Ces journaux d'audit fournissent à un administrateur des données d'analyse sur les changements apportés par des utilisateurs auxquels des pouvoirs ont été délégués. L'administrateur peut les utiliser pour suivre les objets Active Directory et les utilisateurs créés, modifiés ou supprimés, ainsi que le technicien ayant effectué l'action. Découvrez ces rapports d'audit en détail en téléchargeant gratuitement la version d'évaluation de l'outil qui permet un accès illimité à toutes ses fonctionnalités de gestion et de suivi.

4.2 Délégation d'autorisations de gestion Active Directory et Office 365

La délégation d'autorisations de gestion et de suivi Active Directory gagne en importance dans les environnements Microsoft Windows. La croissance d'une organisation entraîne le développement de son réseau, d'autres ressources et des tâches administratives à un rythme accéléré. Il devient difficile pour la DSI de gérer tout l'environnement Active Directory de façon rapide, fiable et efficace. Le fait que les administrateurs informatiques doivent suivre une longue liste de bonnes pratiques pour déléguer la gestion Active Directory aggrave la situation. Les outils natifs rendent la délégation Active Directory lourde et complexe.

ADManager Plus, solution Web de gestion Active Directory, offre la capacité indispensable de déléguer des tâches de gestion courantes pour Active Directory, Exchange, Office 365 et Google Workspace à des utilisateurs autres que les administrateurs avec ses outils de pointe. La solution permet à un administrateur AD de déléguer des tâches à des utilisateurs standards comme les techniciens d'assistance avec des contrôles d'authentification et d'autorisation adéquats, ce qui réduit nettement la charge d'administration.

4.3 Réception d'alertes en temps réel sur des actions de gestion AD

Un environnement Active Directory (AD) connaît souvent de nombreux changements. De plus, s'il existe plusieurs administrateurs AD, il faut avertir tous les intéressés à l'exécution d'une tâche afférente.

ADManager Plus fournit des alertes en temps réel par courrier ou SMS chaque fois qu'on exécute une tâche de gestion AD avec le produit.

Profils de notification personnalisés

Créez des profils de notification selon :

- La ou les actions effectuées.
- Domaine.
- Technicien d'assistance ayant effectué l'action.

Recevez des notifications lorsque :

- Des utilisateurs sont créés ou modifiés.
- Des attributs généraux et Exchange sont modifiés.
- Des ordinateurs sont créés ou modifiés en masse.
- Des contacts sont créés ou modifiés en masse.

- Des groupes sont créés ou modifiés en masse.
- Des boîtes aux lettres partagées et de ressources sont créées ou modifiées.
- Des OU sont créées ou modifiées.
- Des licences d'utilisateur Office 365 sont affectées ou retirées.
- Des comptes Office 365 sont créés pour des utilisateurs AD existants.
- Des tâches Exchange Online sont exécutées.

Modèles de notification

Utilisez des modèles de notification existants ou créez-en pour personnaliser vos notifications par courrier ou SMS. Créez des modèles de notification flexibles qui permettent à la fois de recevoir des alertes sur l'exécution de tâches de gestion AD et d'informer les utilisateurs ou d'autres intéressés.

À la prochaine exécution d'une tâche de gestion AD, Exchange ou Office 365 dans l'organisation avec ADManager Plus, vous êtes immédiatement averti.

Souhaitez-vous des notifications sur les tâches en attente d'exécution ? Utilisez des règles de notification de workflow pour prévenir les intéressés des demandes liées à AD créées, examinées ou approuvées.

ADManager Plus est une solution Web pour tous les besoins de gestion AD, Office 365 et Exchange. Elle simplifie les tâches courantes comme l'attribution d'utilisateurs, le nettoyage de comptes inactifs, la gestion des autorisations NTFS et de partage, etc. ADManager Plus offre aussi plus de 150 rapports prédéfinis, notamment sur les comptes d'utilisateur AD inactifs ou verrouillés, les licences Office 365 et les heures de dernière connexion réelle des utilisateurs. Exécutez des tâches de gestion directement à partir de rapports. Créez un cadre de workflow personnalisé pour faciliter la gestion des tickets et la conformité ou automatiser des tâches AD courantes comme l'attribution d'utilisateurs et la désactivation.

4.4 Suivi des techniciens d'assistance

Obtenez une liste complète de toutes les actions AD réalisées par des techniciens pour réussir des audits de conformité.

4.5 Journal d'audit des techniciens d'assistance

Le journal d'audit des techniciens d'assistance est une fonction d'accessibilité visant à permettre aux auditeurs/administrateurs d'assurer un suivi détaillé de l'activité du système ADManager Plus.

Un journal d'audit est un fichier/document qui conserve les détails de toutes les tâches de gestion AD comme la réinitialisation de mot de passe, la suppression d'utilisateur, la création/modification de compte d'utilisateur, etc., effectuées avec ADManager Plus.

Les journaux d'audit s'avèrent pratiques, car on peut effectivement examiner l'auteur d'une action et le moment tout en détectant des problèmes/erreurs liés aux tâches ayant échoué. Les journaux résident dans des dossiers distincts en rapport avec l'utilisateur concerné qui a effectué la tâche. Cet outil commode permet et facilite un examen chronologique de l'activité de gestion AD.

Un journal d'audit contient en fait ces détails sur chaque tâche réalisée :

- Auteur de la tâche

Le journal d'audit consigne les détails de la personne qui a effectué une tâche de gestion AD. Si un administrateur a réalisé la tâche, le journal est stocké dans le volet admin du dossier de technicien. Pour un technicien d'assistance, le journal est stocké dans un dossier dont le nom correspond au technicien et au domaine associé. Par exemple, Jean-ADMP signifie que ce dossier contient les journaux générés alors que le technicien d'assistance Jean exécutait des tâches de gestion AD dans le domaine ADMP.

- Moment de la tâche

Le journal d'audit enregistre la date et l'heure d'un événement. Cette information s'avère utile pour déterminer ensuite le moment où a lieu une tâche de gestion AD.

- Action de la tâche

Le journal d'audit consigne les détails de la tâche effectuée au déclenchement de l'événement. Il enregistre les détails de tous les attributs dont les valeurs sont mises à jour pour référence ultérieure. Par exemple, si on transfère un utilisateur d'une unité d'organisation à une autre avec ADManager Plus, le journal d'audit généré contient les détails des OU source et cible sous les titres respectifs De et À.

Archivage de rapports d'audit d'assistance

On peut archiver des rapports d'audit pour les extraire ensuite à des fins de conformité à des exigences légales ou une stratégie d'entreprise. ADManager Plus permet à un administrateur de personnaliser l'intervalle d'archivage, la période de rétention et l'emplacement des archives. On peut extraire les archives en choisissant celle voulue dans la liste, le technicien d'assistance ou la période pour laquelle on a archivé le rapport d'audit. On peut exporter les rapports aux formats CSV, XLSX, PDF et HTML.

Les rapports d'audit donnent les détails d'une tâche de gestion AD réalisée par un technicien avec AD Manager Plus. Ces rapports assurent un suivi de l'état de la tâche/opération effectuée par le technicien, du nom de l'objet ou de la catégorie d'action pour permettre un contrôle étroit des événements comme la réinitialisation de mot de passe, la suppression d'utilisateur, la création/modification de compte d'utilisateur, etc. Les rapports d'audit affichent le module utilisé par le technicien d'assistance (par exemple, Automatisation ou Gestion AD) pour réaliser les tâches attribuées.

4.6 Délégation de sécurité Active Directory

ADManager Plus utilise une gestion des autorisations basée sur le rôle pour une administration Active Directory efficace. Un rôle est un regroupement logique d'autorisations pour des tâches courantes d'administration de la sécurité. Des listes de contrôle d'accès (ACL) contiennent les autorisations liées aux objets Active Directory. Les entrées de contrôle d'accès (ACE) d'un objet déterminent les principaux de sécurité et les autorisations afférentes.

La création de rôles de sécurité est bien plus simple que la gestion de listes de contrôle d'accès. On peut déléguer facilement et logiquement les rôles de sécurité à plusieurs utilisateurs, ordinateurs ou à un groupe. Cela minimise les erreurs et assure l'uniformité dans la délégation

d'autorisations de sécurité outre le fait de simplifier et d'améliorer le processus. Tel n'est pas le cas si on tente d'effectuer la délégation avec les outils AD natifs ou PowerShell.

Délégations prêtes à l'emploi

ADManager Plus intègre les rôles de sécurité que l'on peut déléguer directement aux principaux de sécurité pour accorder l'autorisation d'effectuer ces tâches d'administration essentielles :

- Réinitialisation de mots de passe d'utilisateur
- Déverrouillage de comptes d'utilisateur
- Ajout de membres à des groupes et suppression
- Transfert d'utilisateurs à une autre OU du domaine
- Transfert d'ordinateurs à une autre OU du domaine
- Ajout de postes de travail au domaine et suppression
- Création de comptes d'utilisateur
- Création, suppression et modification d'attributs de compte d'utilisateur

Recherche d'ACE

ADManager Plus permet de rechercher les autorisations accordées aux principaux de sécurité comme des utilisateurs, des groupes ou des ordinateurs. La solution offre l'option d'inclure l'objet Active Directory, le principal de sécurité et les autorisations dans les critères de recherche.

5 Workflow

5.1 Exécution normalisée des tâches AD

Analysez et simplifiez les tâches AD dans toute votre organisation grâce à des workflows à approbation.

5.2 Création de workflows personnalisés pour des besoins précis. Flux de travail Active Directory
Dans le monde actuel des technologies de l'information, Active Directory fonctionne comme une ruche pour toutes les activités d'une organisation. Ainsi, un seul faux pas peut déclencher une série de catastrophes en cascade, susceptible d'aboutir à l'effondrement total des fonctions de l'organisation.

Afin d'éviter de telles conséquences, l'équipe de gestion d'Active Directory doit prendre des mesures de sécurité et veiller à ce que toutes les actions effectuées dans AD soient supervisées ou vérifiées en double.

Les administrateurs conviendront que cette fonction n'est pas si facile, surtout lorsqu'on utilise des options conventionnelles comme les outils AD natifs, PowerShell, etc., en raison de la complexité, des heures de travail et des autres ressources nécessaires pour sécuriser Active Directory. Pour pallier à ces difficultés, ADManager Plus vous propose un Workflow - un système de gestion des flux de travail, d'administration des incidents Active Directory et de conformité, au sein même d'ADManager Plus !

Flux de travail Active Directory

Le flux de travail est un peu comme un référentiel pour les demandes de tâches ou les tickets Active Directory, qui permet également à l'administrateur de définir le flux d'approbation pour spécifier comment les tâches de gestion comme la création, la modification de comptes, le nettoyage d'Active Directory, etc. doivent être exécutées.

Fonctionnalités :

- La possibilité de construire une structure de flux de travail personnalisée, avec le nombre requis d'agents de workflow en fonction des besoins de l'organisation. à savoir le demandeur, l'examineur, l'approbateur et l'exécuteur.
- Référentiel de demandes pratiquement illimité. Tous les agents présents dans la boucle peuvent afficher toutes les demandes, suivre celles qui ont été traitées et y donner suite (s'ils sont désignés pour le faire).
- Fonctionne comme une boîte à outils de conformité ; avec une liste exhaustive de toutes les demandes traitées, qui peut être conservée pendant une période donnée ou aussi longtemps que vos lois de conformité informatique l'exigent
- Facilite la notification aux utilisateurs concernés à tout moment pendant l'exécution d'une tâche
- La possibilité de définir un ensemble de règles qui permettent d'attribuer un ensemble d'agents de workflow et une priorité à une tâche spécifique
- Le flux de travail peut également être mis en œuvre dans l'automatisation d'ADManager Plus afin de conserver le niveau de contrôle requis sur les tâches automatisées.

5.3 Auto-affectation de tâches AD à des techniciens

Établissez des règles pour affecter automatiquement des tâches à des techniciens selon l'action, le domaine ou la priorité.

5.4 Utilisation du workflow AD comme outil de conformité informatique

Un workflow permet de créer la séquence du flux d'une tâche organisationnelle et de définir les agents le composant. Il prend en charge les transferts et les transmissions intermédiaires. Son référentiel des demandes tient informé de l'état des tâches en cours.

Workflow personnalisable

ADManager Plus, contrairement aux outils natifs ou PowerShell, permet de définir une structure de workflow standard pour toutes les tâches organisationnelles.

Elle peut comporter jusqu'à quatre niveaux d'agents de workflow : demandeurs, examinateurs, approbateurs et exécuteurs. Elle sert de feuille de route bien établie pour toutes les tâches. Une structure de workflow claire élimine tout risque de conflits de rôles. Les communications et les informations restent en sécurité, car elles ne circulent qu'entre les destinataires prévus.

Référentiel des demandes

ADManager Plus conserve une liste complète de toutes les demandes ouvertes et terminées. On dispose d'informations détaillées sur une tâche créée pour exécution, notamment l'heure à laquelle l'exécution a commencé, le demandeur, les agents de workflow désignés et l'état de workflow de cette tâche. ADManager Plus assure un suivi électronique de toutes les tâches exécutées et des accès effectués, pour faciliter la conformité à des réglementations comme SOX.

Règles d'affectation

Les règles d'affectation et de notification intégrées à un workflow ADManager Plus permettent de définir des règles conditionnelles selon lesquelles affecter un technicien ou une priorité à une tâche. ADManager Plus permet aussi de classer ces règles pour prioriser leur application à une tâche. On peut avertir les agents de workflow des demandes créées, examinées ou approuvées. Essentiellement, cela associe le type d'action (création, examen, approbation ou exécution d'une demande) à des agents de workflow à des fins de notification. Cela permet enfin de communiquer cette information à des techniciens et d'autres intéressés via des courriers et des messages.

Automatisation de tâches cruciales

Des tâches courantes simples comme la création d'utilisateurs ou la suppression/désactivation d'utilisateurs inactifs s'avèrent parfois cruciales pour le bon fonctionnement d'une organisation. On peut donc traiter ces tâches courantes avec l'automatisation ADManager Plus pour l'efficacité opérationnelle. Certaines de ces tâches s'avérant cruciales, il est probable que le maintien d'un certain degré de contrôle sur l'automatisation devienne nécessaire. On y parvient

facilement en déployant le workflow fonctionnel pour l'automatisation. On assure ainsi l'exécution de la tâche automatisée sous la supervision des agents du workflow fonctionnel.

- Création de demandes de workflow pour accorder ou modifier des autorisations de dossier partagé
- Modification d'autorisations NTFS en masse

Points forts

- Workflow linéaire facilitant l'affectation et la priorisation des tâches
- Impossibilité de contourner le workflow, d'où une haute sécurité et transparence
- Système de suivi de l'état des tâches en ligne
- Catalogue des rôles de l'organisation et des tâches
- Enregistrement des tâches et des données Active Directory pour extraction à tout moment
- Possibilité de déploiement pour superviser des tâches automatisées

5.5 Prévention des modifications AD non autorisées

Analysez les opérations AD afin qu'elles respectent les normes de sécurité de votre organisation.

5.6 Affichage du statut des tickets en temps réel

Recevez des notifications par e-mail ou SMS après chaque étape de traitement d'une demande (par exemple, à sa création, son examen, son approbation ou son exécution).