

CAS D'UTILISATION 5

Remote Desktop Manager + Devolutions Server

Utiliser Devolutions Server pour améliorer la sécurité lors de l'authentification des utilisateurs de Remote Desktop Manager

Comment renforcer la sécurité en n'exposant pas la base de données pendant le processus d'authentification des utilisateurs de Remote Desktop Manager

Le public cible

Ce cas d'utilisation s'adresse aux organisations qui souhaitent renforcer la sécurité en empêchant l'exposition de leur base de données pendant le processus d'authentification des utilisateurs de Remote Desktop Manager.

L'enjeu

Remote Desktop Manager est une solution sécurisée qui permet d'authentifier chaque utilisateur. Elle empêche les connexions non autorisées et facilite les processus d'audit.

L'une des méthodes que Remote Desktop Manager prend en charge pour l'authentification des utilisateurs est la connexion à une base de données SQL. Cette méthode est rapide et pratique. Par contre, elle ouvre également la porte à des problèmes de sécurité potentiels, parce qu'elle permet aux utilisateurs finaux de se connecter directement à la base de données à l'aide d'un outil facilement accessible comme Excel ou SQL Server Management Studio (SSMS). Dans certaines organisations, cette situation est inacceptable d'un point de vue de conformité.

La solution

Cette faille de sécurité n'est pas due à Remote Desktop Manager, mais plutôt à la connexion externe avec la base de données SQL. Elle peut être éliminée en utilisant **Devolutions Server**. Il s'agit de notre solution de gestion de mots de passe et de comptes partagés, qui inclut des composants de gestion d'accès privilégiés répondant aux exigences de sécurité toujours croissantes des organisations, y compris des PME.

Devolutions Server fournit à chaque utilisateur final une identité dédiée et unique, soit par le biais du répertoire Active Directory, soit par Microsoft Office365. Ainsi, les utilisateurs finaux n'ont jamais accès à la base de données pendant le processus d'authentification de Remote Desktop Manager. Le processus est transparent et les utilisateurs finaux continuent de bénéficier d'une connexion rapide et d'une expérience conviviale.

Le fonctionnement

Étape 1: [Téléchargez et installez Devolutions Server.](#)

Étape 2: [Créez des groupes AD](#) spécifiques pour accéder à **Devolutions Server** et ajoutez vos utilisateurs finaux à ces groupes.

Étape 3: À partir de l'interface Web de Devolutions Server, [configurez les groupes AD](#). Une fois que les utilisateurs y seront ajoutés (voir l'étape suivante), ils auront une identité dédiée et unique qui sera utilisée à des fins d'authentification.

Étape 4: Créez vos utilisateurs AD en les [important](#) ou en demandant à vos utilisateurs de se connecter via l'interface Web.

Résumé des avantages

- **Renforce la sécurité :** éliminez la possibilité que les utilisateurs finaux accèdent à la base de données pendant le processus d'authentification de Remote Desktop Manager.
- **Assure la conformité :** respectez les règles et réglementations de la sécurité de l'information requises.
- **Améliore la gestion des utilisateurs :** bénéficiez d'un meilleur contrôle et d'une surveillance accrue du roulement de personnel et de la suppression des accès.

Prochaines étapes

Découvrez comment Devolutions peut aider votre organisation à renforcer la sécurité et améliorer la gestion des utilisateurs, tout en assurant la conformité.

- **Demandez un essai gratuit de Devolutions Server** – [cliquez ici](#)
- **Demandez un essai gratuit de Remote Desktop Manager** – [cliquez ici](#)
- **Demandez une démonstration en direct de Remote Desktop Manager** – [cliquez ici](#)
- **Communiquez avec nous pour plus d'informations** – [cliquez ici](#)