Bureaux à distance : sécurité et gestion des mots de passe

Petri IT Knowledgebase
Une propriété BWW Media Group

Commandité par
Devolutions

Michael Otey

Michael Otey est président de TECA, inc., une entreprise que se spécialise dans la consultation et le développement de produits Windows et SQL Server. Il contribue régulièrement à des publications techniques et il est l'auteur de plusieurs ouvrages sur le développement et la programmation de bases de données.

De nos jours, la gestion des bureaux à distance est une des activités principales des administrateurs TI et le Bureau à distance est, pour eux, un outil incontournable. Le Bureau à distance permet de démarrer une session interactive avec un système distant et de le contrôler comme s'il s'agissait d'un système local. Les connexions de Bureau à distance sont essentielles pour une gestion et un dépannage à distance efficaces. S'il s'agit d'un outil indispensable, il faut aussi rappeler qu'il s'agit d'une application très puissante qui doit être sécurisée.

Les connexions à distance ont souvent des privilèges élevés, parce qu'elles doivent effectuer différentes tâches administratives. Cela signifie qu'il est essentiel que votre plateforme de gestion des connexions à distance soit sécurisée. Les administrateurs et les utilisateurs utilisent différents navigateurs Web pour plusieurs tâches quotidiennes. De nombreux sites Web nécessitent des informations d'identification qui doivent, elles aussi, être sécurisées.

Dans ce document technique, vous découvrirez certains défis liés la gestion des mots de passe et des bureaux à distance. Vous verrez aussi comment vous pouvez utiliser **Remote Desktop Manager (RDM)** de Devolutions pour gérer de manière centralisée et sécurisée des mots de passe de vos utilisateurs privilégiés et finaux dans la même plateforme.

Gestion des mots de passe : les défis

La gestion des mots de passe est un défi constant pour les départements et organisations du monde entier. La sécurisation des mots de passe, en particulier administratifs, est vitale pour la sécurité d'une entreprise. Ils représentent la première ligne de défense pour protéger les actifs de l'entreprise et pour permettre aux utilisateurs d'être productifs. Les mots de passe exposés peuvent entraîner des violations de données, des piratages, des menaces internes et même exposer vos données et des informations commerciales critiques à des logiciels malveillants et des rançongiciels. Voici quelques-uns des principaux défis en matière de gestion des mots de passe :

- **Garder les mots de passe des employés confidentiels** – Le premier défi de la gestion des mots de passe est de s'assurer qu'ils sont réellement secrets. Les utilisateurs sont connus pour être assez laxistes avec la sécurité de leurs mots de passe. Ils les partagent, utilisent des notes autocollantes pour les afficher sur leurs moniteurs et utilisent des mots de passe très faibles tels que « mot de passe ».

- **Partage de comptes privilégiés** – Les utilisateurs ne sont pas seuls à créer des risques de sécurité avec leurs mots de passe. Plusieurs administrateurs partagent des comptes administratifs privilégiés, simplement parce que ça se fait ainsi depuis longtemps. Cette pratique peut effectivement faciliter certaines tâches, mais elle élimine également la possibilité d'archiver et d'auditer les modifications.

• **Réutilisation de noms de comptes et de mots de passe communs** – Un autre défi de sécurité consiste à empêcher les utilisateurs de réutiliser des noms de comptes et des mots de passe courants. Si vous visitez de nombreux sites Web ou vous devez avoir accès à un grand nombre de systèmes distants, il peut être tentant d'utiliser les mêmes informations de connexion. Cette pratique n'est pas sécuritaire et si l'un des sites est compromis, ceux qui utilisent les mêmes informations de connexion pourraient l'être également.

• **Ne pas changer les mots de passe par défaut** – Un autre problème potentiel est de négliger de changer les mots de passe par défaut qui sont fournis avec certaines applications et appareils. Ces mots de passe ne sont généralement pas très forts et ils sont bien connus. Négliger la modification de ces mots de passe peut vous exposer à des problèmes de sécurité.

• **Les attaques d'ingénierie sociale** – Les attaques d'hameçonnage sur les réseaux sociaux et par courriel, conçues pour inciter les utilisateurs à fournir des informations de connexion, constituent un autre défi en gestion de mots de passe. Les informations recueillies par les pirates sont utilisées pour accéder aux ressources de votre entreprise.

• **Protection contre le piratage de mots de passe** – Un autre défi consiste à empêcher le vol de mots de passe par des programmes qui vont décrypter/trouver des mots de passe. Les mots de passe sont généralement stockés dans un hachage cryptographique sur les systèmes auxquels vous accédez. Si le pirate peut accéder au fichier de hachage, par exemple en obtenant une copie des fichiers VHD d'une machine virtuelle, il peut utiliser différents programmes pour tenter d'extraire les informations de sécurité de votre organisation. Le stockage des mots de passe dans des emplacements sécurisés, l'utilisation de mots de passe forts et la conservation de mots de passe séparée pour différents systèmes peuvent aider à atténuer cette menace.

• **La difficulté d'effectuer des audits pour les comptes privilégiés** – La possibilité d'archiver et de suivre les actions de vos administrateurs peut être particulièrement importante pour auditer les accès à distance et être en mesure d'identifier la personne responsable d'un ensemble de modifications.

• **Manque de gestion centralisée** – Sans gestion centralisée, des mots de passe importants peuvent être distribués dans de nombreux endroits de l'organisation, ce qui affaiblit la sécurité du réseau et augmente les efforts de gestion et d'assistance qui doivent être déployés. La gestion centralisée des mots de passe réduit l'exposition et offre un outil simple pour gérer vos informations d'identification à distance.

Il est essentiel de sécuriser correctement vos connexions à distance, parce qu'elles peuvent exposer l'entreprise à des failles de sécurité. RDM de Devolutions fournit plusieurs fonctionnalités de sécurité de base pour les entreprises qui peuvent vous permettre de sécuriser et de gérer de manière centralisée l'accès aux différents serveurs à distance de votre organisation.

Gestion sécurisée des mots de passe via Remote Desktop Manager

Les mots de passe constituent la base de votre stratégie de sécurité à distance et RDM fournit plusieurs fonctionnalités de base qui vous permettent de mieux contrôler et sécuriser les mots de passe utilisés par les utilisateurs. Il prend en charge les politiques de mot de passe, la génération et l'application des mots de passe ainsi que la gestion centralisée des mots de passe à distance.

Politiques de mot de passe dans RDM

Des politiques de mot de passe strictes sont votre première ligne de défense contre les failles de sécurité. Bien que la plupart des utilisateurs et administrateurs réalisent que des mots de passe forts sont importants, il est facile d'être laxiste ou frustré par ceux-ci lorsque vous travaillez avec de nombreux sites à distance. Des politiques de mots de passe centralisées peuvent empêcher les utilisateurs d'utiliser des mots de passe faibles. RDM prend en charge toutes les politiques de mot de passe essentielles pour appliquer des mots de passe forts, comme:

- **Une longueur minimale du mot de passe** – Nécessite un nombre minimal de caractères dans un mot de passe.
- **Des exigences de complexité** – Garantit que le mot de passe ne peut pas contenir le nom d'utilisateur et qu'il doit utiliser au moins trois des quatre types de caractères possibles : lettres minuscules, lettres majuscules, chiffre et symboles.
- **L'historique des mots de passe** – Empêche la réutilisation de l'ancien mot de passe pendant une période spécifiée.
- **L'âge du mot de passe** – Exige qu'un utilisateur change son mot de passe après une période donnée.

Lorsque vous fournissez des mots de passe pour vos sessions à distance dans RDM, l'analyseur de mots de passe évaluera automatiquement les mots de passe et vous mentionnera s'ils sont forts ou faibles.

Il est recommandé de mettre en oeuvre une politique d'ancienneté des mots de passe qui oblige les utilisateurs à modifier leurs mots de passe forts tous les 90 jours et leurs phrases secrètes tous les 180 jours. RDM vous permet de créer une liste de mots de passe interdits qui peuvent empêcher les utilisateurs de créer des mots de passe facilement devinables comme « mot de passe ».

Générateur de mots de passe

Créer un mot de passe fort peut être une tâche laborieuse pour certains utilisateurs. Pour rendre cette tâche plus facile et sécuritaire, RDM fournit un générateur de mot de passe intégré à chaque entrée de session. Le générateur de RDM est capable de créer des mots de passe aléatoires complexes hautement sécurisés. Vous pouvez créer les mots de passe à l'aide du modèle de création par défaut ou vous pouvez créer vos propres modèles de génération personnalisés. Vous pouvez voir le générateur de mots de passe RDM dans la figure 1. La partie inférieure de la fenêtre affiche la liste des mots de passe générés. Chacun d'entre eux peut avoir un niveau de force différent allant de très fort à parfait. Cliquez sur un mot de passe, puis cliquez sur le bouton « Sélectionner ». Cela insérera le mot de passe généré automatiquement.

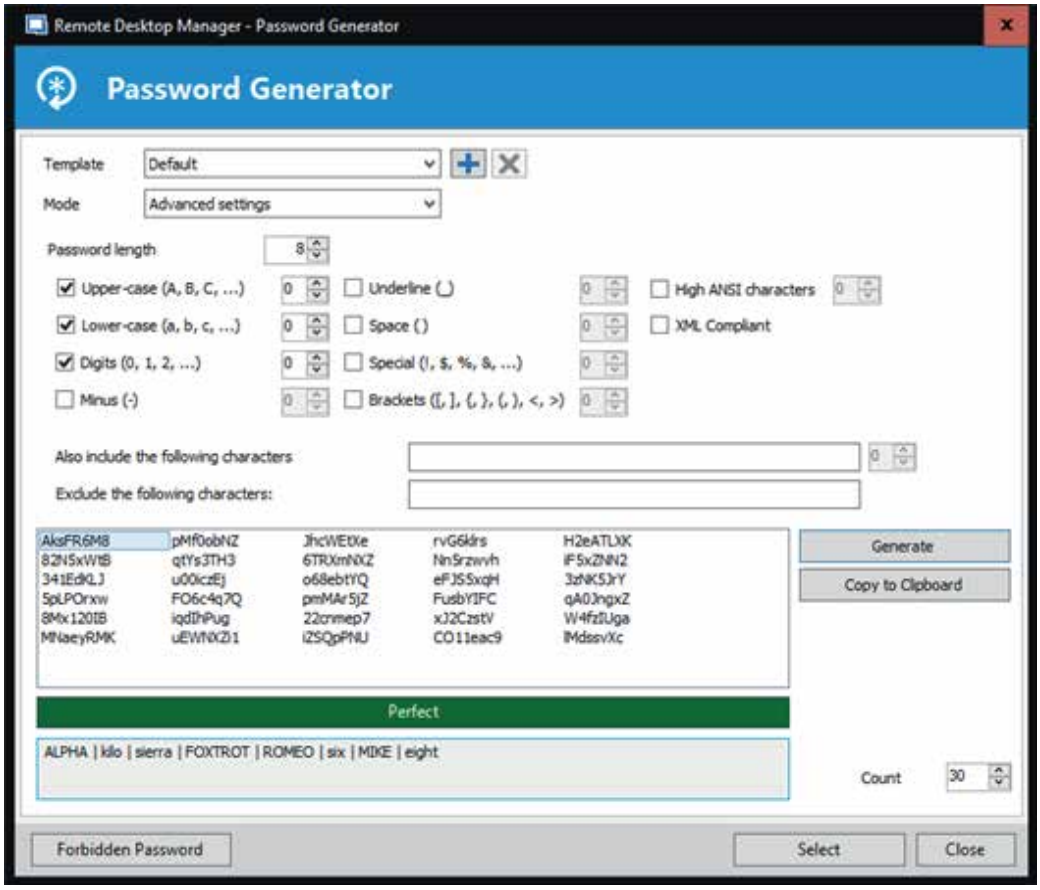

Figure 1 - Création automatique de mots de passe forts avec le générateur de mots de passe de RDM

Analyseur de mot de passe

Pour permettre aux administrateurs de vérifier périodiquement la force des mots de passe utilisés, RDM fournit un analyseur intégré qui peut évaluer les mots de passe utilisés par tous les utilisateurs de chaque session à distance. Vous pouvez voir un exemple de l'analyseur de mots de passe de RDM dans la figure 2. Vous pouvez aussi voir que les mots de passe pour chaque session et utilisateur sont classés comme faibles, forts, très forts et parfaits. Double-cliquez sur l'une des entrées pour afficher la boîte de dialogue de configuration de session. Cela vous permet de changer le mot de passe pour les sessions qui ont des mots de passe faibles.

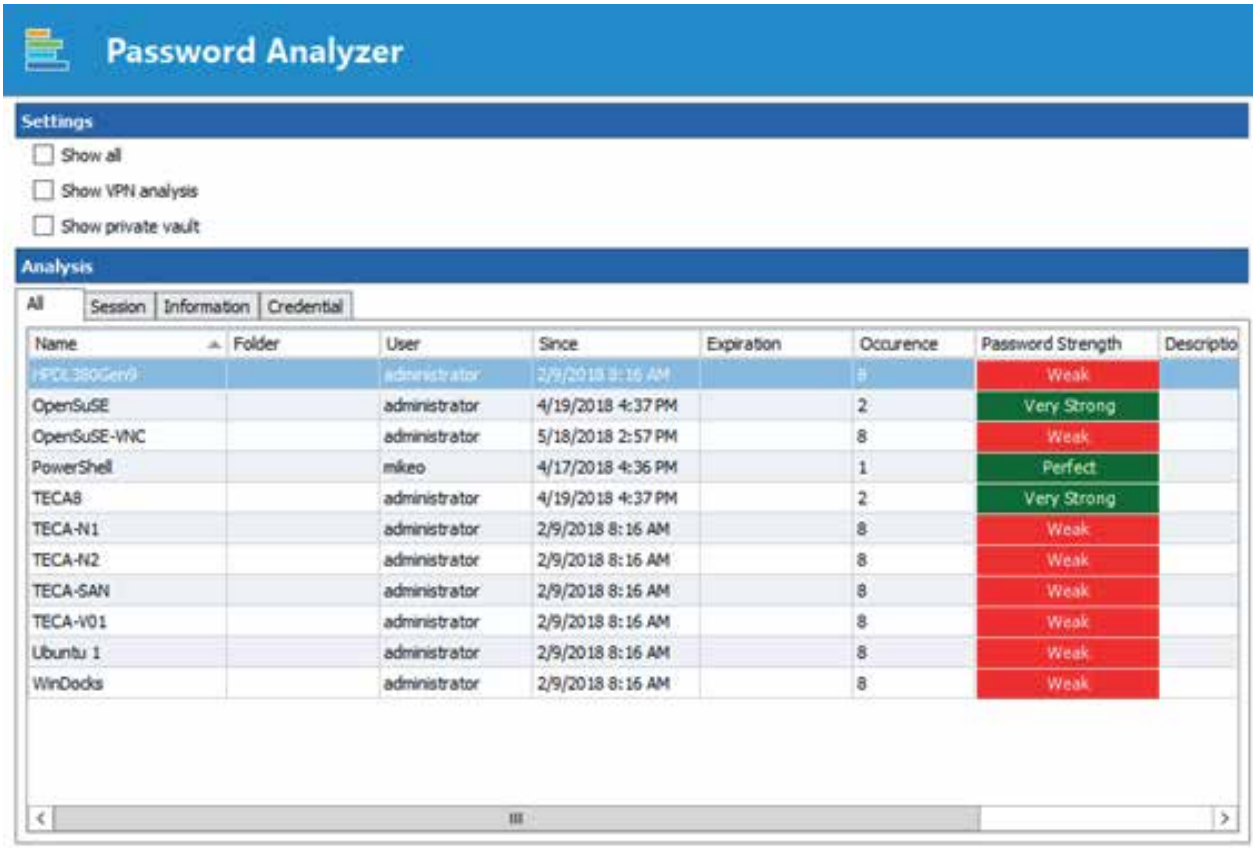

Figure 2 - L'analyseur de RDM peut signaler des mots de passe faibles.

Gestion centralisée des mots de passe

Les administrateurs TI sont responsables de la gestion et du contrôle de l'accès aux différents serveurs sur site et hors site. Cependant, l'accès à distance pour de nombreuses entreprises est généralement inefficace et non sécurisé, puisqu'il repose sur plusieurs outils de connexion à distance et souvent sur de nombreux gestionnaires de mots de passe différents. RDM peut résoudre le problème de l'accès à distance sécurisé en offrant la possibilité de gérer de manière centralisée et sécurisée tous vos mots de passe de connexion à distance. RDM peut stocker les mots de passe à l'échelle de l'entreprise dans une base de données chiffrée sur site, ce qui aide les utilisateurs à accéder rapidement aux informations de connexion et à les partager entre les utilisateurs et entre les équipes. Vous pouvez configurer plusieurs connexions à distance partagées à partir d'un répertoire centralisé fournissant des connexions sécurisées aux serveurs distants, aux machines virtuelles, aux sites Web et aux applications. RDM prend en charge un large choix de technologies, notamment Remote Desktop Protocol, RemoteFX, RealVNC, TightVNC, UltraVNC, Citrix ICA, LogMeIn, TeamViewer, RGS, DameWare, Radmin, pcAnywhere, Telnet, VMware vSphere, Hyper-V et plus. RDM simplifie l'accès à distance en consolidant plusieurs types de connexions dans une seule fenêtre, ce qui réduit l'encombrement du bureau et fournit un portail d'accès à distance unique.

En plus de gérer les connexions de bureaux à distance, RDM fournit un accès sécurisé centralisé aux sites web avec son extension de navigateur. Devolutions Web Login peut stocker et récupérer les informations d'identification requises pour vous connecter à n'importe quel site web. Cette technologie fonctionne avec RDM pour obtenir des informations d'identification et remplir automatiquement tous les champs d'authentification affichés.

Les informations d'authentification sont automatiquement remplies lorsque vous utilisez RDM pour accéder à un site web. Vous pouvez voir un exemple de création d'une nouvelle connexion web dans la figure 3.

Dans la figure 3, vous pouvez voir comment l'entrée de connexion web stocke l'URL, puis les informations de connexion pour un site internet distant qui nécessite une authentification. Tout comme les connexions de bureau à distance, le site web peut être affiché comme ancré dans la fenêtre principale RDM ou être affiché en mode désancré sur le bureau. Cocher le lien « Activer l'extension du navigateur web » permet à RDM de transmettre les informations de connexion au navigateur.

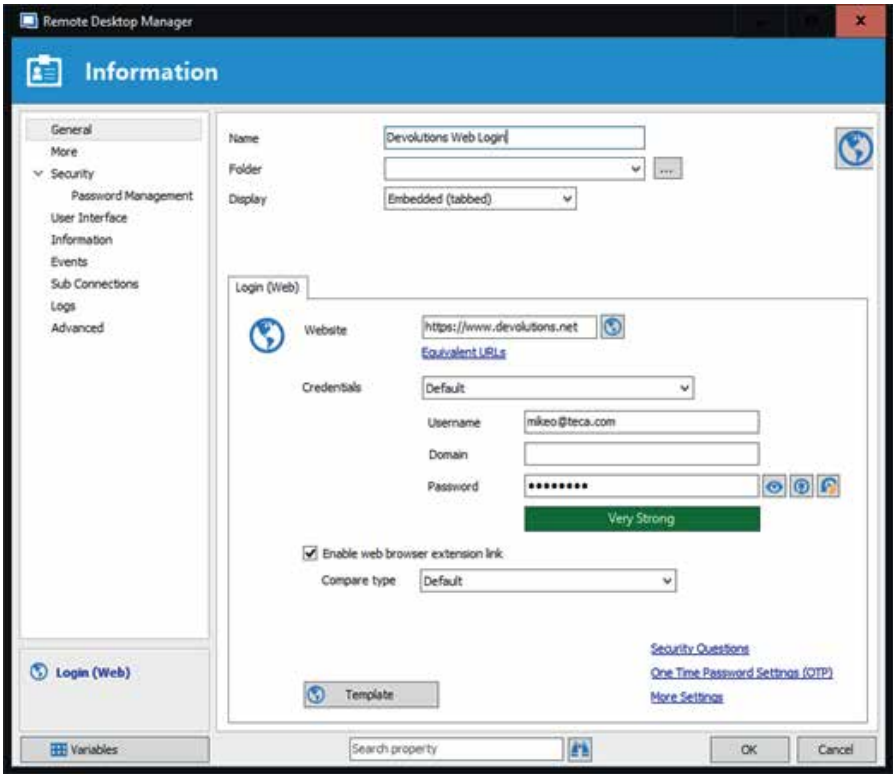

Figure 3 - Création d'entrées de connexion web

La sécurité basée sur les rôles

Pour faciliter et contrôler l'accès à distance pour plusieurs utilisateurs, RDM offre une gestion basée sur les rôles qui permet à l'administrateur de contrôler, déléguer et filtrer l'accès de différents utilisateurs aux comptes privilégiés. Cette fonctionnalité est souvent utilisée pour attribuer différents rôles de sécurité à différents types d'utilisateurs tels que les administrateurs, le personnel du service d'assistance et les consultants. Seuls les utilisateurs autorisés peuvent avoir accès pour afficher, modifier ou gérer les comptes privilégiés autorisés. Les restrictions sont appliquées en fonction des rôles utilisateur prédéfinis. Comme vous vous en doutez, pour utiliser la sécurité basée sur les rôles, vous devez utiliser l'une des sources de données d'équipe partagées comme Microsoft SQL Server, SQL Azure ou Devolutions Server.

La sécurité basée sur les rôles de RDM fonctionne selon des paramètres de sécurité hérités. Les éléments et dossiers enfants sont automatiquement couverts par les paramètres de sécurité d'un dossier parent. Les autorisations spécifiques pour un élément donné peuvent être remplacées. Vous pouvez définir des permissions sur un sous-dossier ou un élément pour remplacer les autorisations de l'élément parent. Toutes les autorisations sont granulaires, ce qui permet de définir plusieurs autorisations sur plusieurs entrées à la fois. La sécurité basée sur les rôles de RDM possède les fonctionnalités suivantes :

- **La sécurité héritée** – Les éléments et dossiers enfants sont couverts par la sécurité du dossier parent.
- **Les autorisations peuvent être remplacées** – L'autorisation définie sur un sous-dossier remplacera les autorisations de l'élément parent.
- **Les autorisations sont granulaires** – Plusieurs autorisations peuvent être définies sur les mêmes entrées.

La sécurité basée sur les rôles profite de l'injection d'informations d'identification lors du partage de sessions pour garantir des connexions à distance sécurisées. Cette injection d'informations d'identification fonctionne à partir de tous les types de connexion, y compris les connexions de bureau à distance et les différentes connexions de sites web. RDM transmet automatiquement les informations d'identification du rôle aux utilisateurs. Ces derniers n'ont jamais accès aux informations d'identification réelles : ils ne sont donc pas en mesure de compromettre les informations de sécurité. Vous pouvez créer de nouveaux rôles à l'aide de l'option « Rôles » du menu Administration de RDM. Vous pouvez voir un exemple de création d'un nouveau rôle avec RDM dans la figure 4.

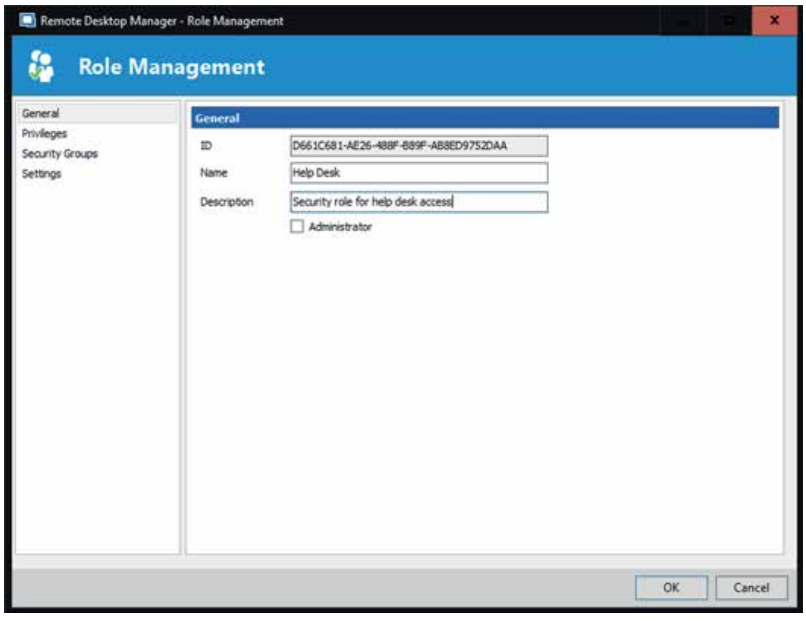

Figure 4 - Création d'un rôle d'utilisateur RDM

Pour créer un rôle, entrez simplement un nom pour le rôle; tous les autres paramètres peuvent être laissés à la valeur par défaut, sauf si le rôle comprend des responsabilités d'administrateur. Si le rôle est octroyé à un administrateur, cochez la case « Administrateur » lorsque vous le créez.

Ensuite, après avoir créé les rôles dont vous avez besoin, vous pouvez attribuer différents utilisateurs aux rôles en cliquant sur l'icône « Rôles » dans la boîte de dialogue « Sécurité et gestion des utilisateurs ». Cela affichera la boîte de dialogue « Attribution de rôle de sécurité » que vous pouvez voir dans la figure 5. Pour attribuer des utilisateurs à un rôle, cochez simplement la case « Est membre » pour l'utilisateur concerné.

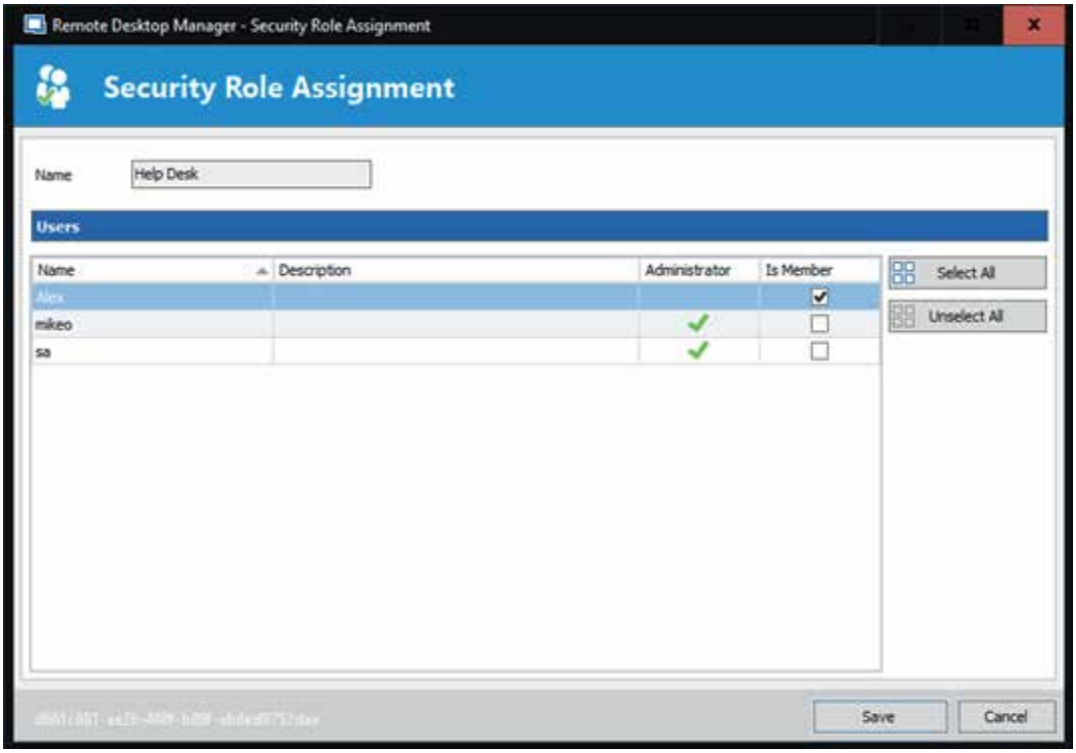

Figure 5 – Attribution de rôles à un utilisateur

Entrées et audit

La journalisation et les rapports d'audit peuvent vous permettre d'évaluer la sécurité de votre organisation et de contrôler l'accès à partir de comptes privilégiés. RDM enregistre toutes les actions pour chaque session et utilisateur. Il fournit également une piste d'audit complète pour la conformité et la création de rapports. RDM enregistre quand les sessions sont ouvertes et fermées, quel utilisateur a effectué l'action et la durée de la session. L'outil capture aussi toutes les opérations de comptes privilégiés, y compris les tentatives de connexion et l'historique. RDM enregistre aussi le moment où les entrées de session sont affichées ou modifiées et qui est derrière cette action. Vous pouvez afficher un rapport des tentatives de connexion infructueuses à un serveur. Vous pouvez voir un exemple de journaux d'activité de connexion à distance de RDM dans la figure 6.

La figure 6 montre l'activité de chaque entrée de session, la date et la durée de la session ainsi que l'utilisateur et le type de session. La fonction de recherche avancée vous permet de filtrer le journal pour des utilisateurs, des événements et des actions spécifiques. Le journal peut également être exporté en fichier CSV pour une analyse plus approfondie.

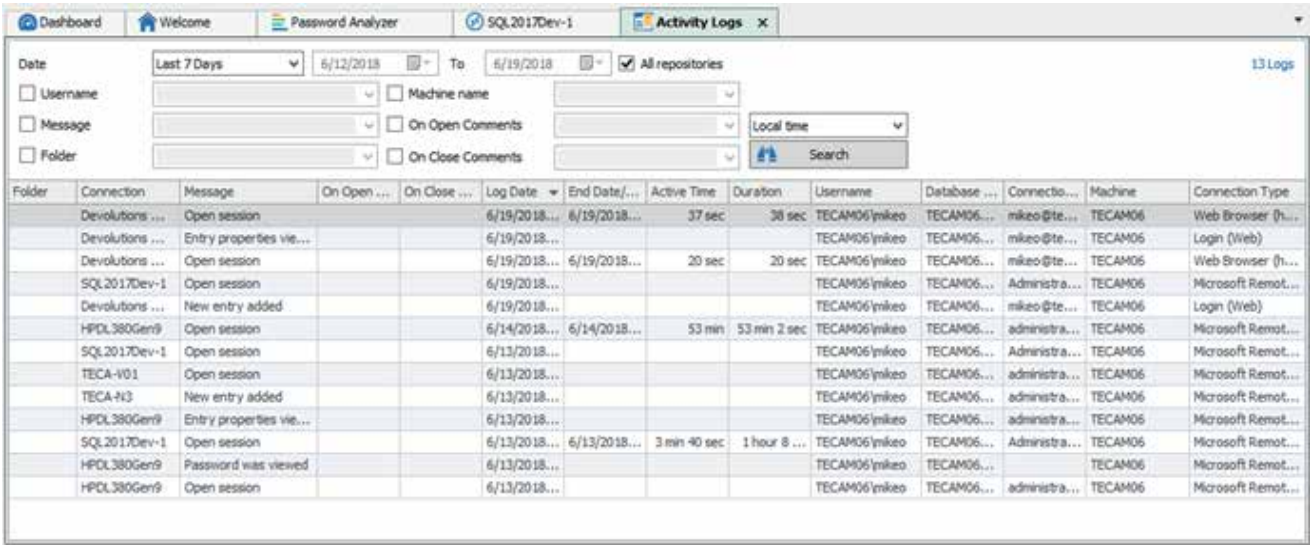

Figure 6 - Affichage du journal d'audit de sécurité de RDM

Considérations supplémentaires sur la sécurité de l'entreprise

RDM fournit également plusieurs autres fonctionnalités de sécurité importantes pour les entreprises. Tout d'abord, il dispose d'une fonction de réservation qui permet à un administrateur de verrouiller l'accès à une session à distance.

Par exemple, si vous exécutiez une maintenance de longue durée et que vous ne vouliez autoriser aucun autre accès au système, vous pourriez quitter la session et les autres utilisateurs ne pourraient pas ouvrir la session jusqu'à ce qu'elle soit restituée. Vous pouvez également restreindre l'accès aux sessions à distance en fonction du temps. Par exemple, vous pouvez uniquement autoriser l'accès à certaines sessions à distance pendant les heures ouvrables.

Pour des exigences de sécurité plus avancées, RDM prend également en charge l'authentification à deux facteurs. L'authentification à deux facteurs est disponible pour les sources de données suivantes : SQLite, Devolutions Server, MariaDB, Microsoft Access, SQL Azure, SQL Server et MySQL.

Gérer les connexions à distance est une tâche complexe et l'utilisation d'outils et de coffres de mots de passe différents peut causer des problèmes de sécurité sans que ce soit votre intention. RDM, avec sa gestion des mots de passe sécurisée et centralisée, peut vous aider à renforcer la sécurité de votre entreprise tout en améliorant la productivité des utilisateurs et administrateurs. La sécurité centralisée basée sur les rôles facilite vos connexions à distance. En outre, la journalisation et l'audit offrent une visibilité sur l'activité des sessions distantes de vos administrateurs et utilisateurs.