Surmonter les défis de la gestion des connexions à distance avec

Remote Desktop Manager

Petri IT Knowledgebase
Une propriété de BWW Media Group

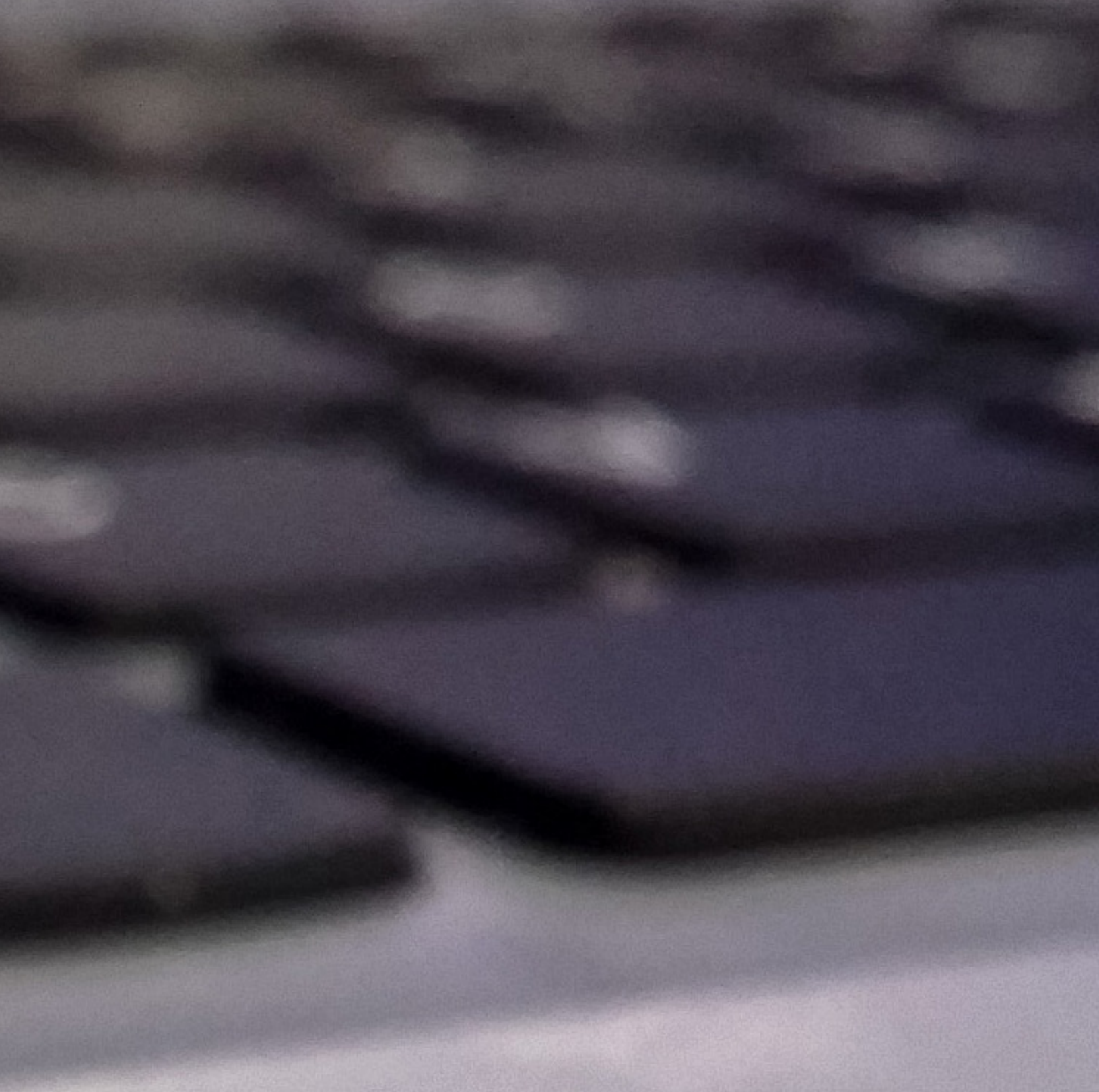
COMMANDITÉ PAR DEVOLUTIONS
Devolutions

Par

Michael Otey

Michael Otey est président de TECA, Inc., une entreprise spécialisée dans le développement de produits Windows et SQL Server et qui offre des services de consultation. Il contribue fréquemment à des publications techniques et est l'auteur de plusieurs livres sur le développement et la programmation de bases de données.

Dans les entreprises d'aujourd'hui, les administrateurs TI doivent généralement gérer de nombreux systèmes distants différents. Ces systèmes peuvent être des systèmes physiques ou des machines virtuelles. Souvent, ces systèmes sont à la fois sur site, à distance et dans le nuage. Les administrateurs Windows utilisent chaque jour des solutions de gestions des bureaux à distance. Elles permettent de démarrer une session interactive avec un système distant. Le gestionnaire de connexions à distance ouvre une fenêtre sur votre système local qui contient le bureau du système distant auquel vous vous connectez. Les actions de votre souris et de votre clavier sont transmises au système distant et la session interactive vous permet d'utiliser et de dépanner le système distant comme si vous étiez assis devant un écran local. Ce type de contrôle et d'affichage interactif est essentiel lorsque vous essayez de résoudre des problèmes ou de configurer des systèmes à distance.



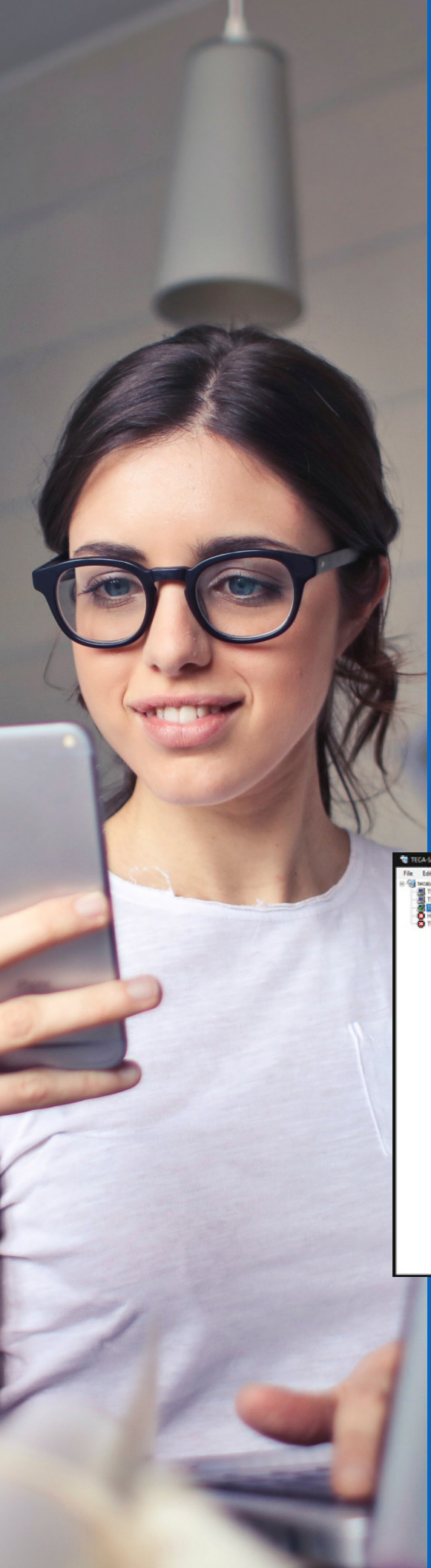
Dans ce livre blanc, vous découvrirez certains des défis liés à l'utilisation des outils de connexion à distance pour gérer les serveurs de votre entreprise, puis vous verrez les meilleurs moyens de résoudre ces problèmes. De nombreuses entreprises utilisent Remote Desktop Connection Manager (RDCman) de Microsoft. Cependant, cet outil de connexion à distance présente plusieurs limites importantes dans un environnement d'entreprise. Vous verrez comment vous pouvez remédier à ces limitations et comment **Devolutions Remote Desktop Manager** offre des fonctionnalités adaptées à l'entreprise pour répondre à vos besoins de gestion des connexions à distance.

LES DÉFIS DE LA GESTION DES CONNEXIONS À DISTANCE

Si la gestion des postes de travail à distance est une tâche quotidienne essentielle, elle peut également causer bien des maux de tête aux administrateurs TI. Examinons de plus près les trois principaux défis de la gestion des bureaux distants.

- **Gérer les connexions multiples** - L'un des plus grands défis est la gestion et l'organisation des connexions distantes multiples. La plupart des administrateurs de PME doivent se connecter à des dizaines, voire des centaines de systèmes distants, ce qui peut être très difficile à gérer. L'utilisation de fichiers RDP vous permet d'enregistrer vos paramètres de connexion et vos identifiants. Cela fonctionne très bien pour quelques systèmes, mais ça devient rapidement très désordonné et potentiellement confus lorsque le nombre de connexions distantes atteint plusieurs dizaines. Tenter de gérer manuellement les connexions peut entraîner un manque d'uniformité, de la confusion et des erreurs potentielles.
- **Sécuriser les connexions à distance -** Le deuxième défi le plus important en matière de gestion des connexions à distance consiste à sécuriser correctement les connexions à distance. Tout comme dans un environnement de bureau traditionnel, les mots de passe constituent la première ligne de défense pour sécuriser l'infrastructure de votre entreprise. Tous les comptes ayant accès aux connexions à distance doivent avoir des mots de passe forts. Pour simplifier la gestion, certaines entreprises tentent d'utiliser les mêmes mots de passe pour plusieurs comptes – ou pire, elles ont recours à des notes autocollantes – ce qui constitue un risque énorme. Vous devez vous assurer que vos connexions au réseau de gestion à distance, de même que vos mots de passe et vos identifiants, sont sécurisés. De plus, lorsque vous devez gérer de nombreux systèmes distants ainsi que des accès pour plusieurs employés TI, vous devez disposer d'un moyen d'enregistrer l'accès à ces systèmes à des fins d'audit et de dépannage.
- **Se connecter à Linux et à d'autres hôtes hétérogènes** - L'un des autres défis est la connexion à des systèmes hôtes hétérogènes. Aujourd'hui, très peu d'entreprises n'ont que des systèmes Windows à gérer. Au contraire, la plupart des entreprises utilisent un mélange de systèmes Windows, Linux, Mac et autres systèmes non Windows. Cela signifie que la plupart des administrateurs Windows doivent utiliser plusieurs outils de gestion à distance. Le Bureau à distance est limité au protocole RDP dont l'utilisation est pratiquement restreinte aux systèmes Windows. Si certaines distributions Linux peuvent être gérées avec RDP, la plupart ne le peuvent pas. L'administrateur doit donc utiliser plusieurs outils comme VNC, Putty et Apple Remote Desktop en plus de Windows Remote Desktop.

Vous pouvez emprunter plusieurs chemins pour surmonter ces obstacles. Vous pouvez essayer d'organiser manuellement plusieurs fichiers .rdp dans des dossiers distincts avec des autorisations différentes, mais ça peut devenir extrêmement lourd et difficile à gérer dans un cas où il y a grand nombre de connexions. Sinon, de nombreuses entreprises choisissent d'utiliser RDCMan ou un gestionnaire de connexions à distance tiers comme Devolutions Remote Desktop Manager pour gérer plus efficacement leurs connexions à distance. Voyons de plus près comment utiliser ces deux solutions.



Remote Desktop Connection Manager de Microsoft

L'un des outils que de nombreux administrateurs informatiques utilisent pour répondre à leurs besoins en matière de gestion des bureaux à distance est RDCMan. Cet outil est téléchargeable gratuitement et peut vous aider à gérer plusieurs connexions à distance en centralisant toutes vos connexions dans une seule console de gestion. RDCMan est pris en charge sur Windows 10 Tech Preview (Windows 10), Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server Tech Preview (Windows Server 2016). RDCMan est un outil de base qui peut vous aider à organiser les connexions distantes sous une seule console. Vous pouvez voir un exemple de Remote Desktop Connection Manager de Microsoft dans la Figure 1.

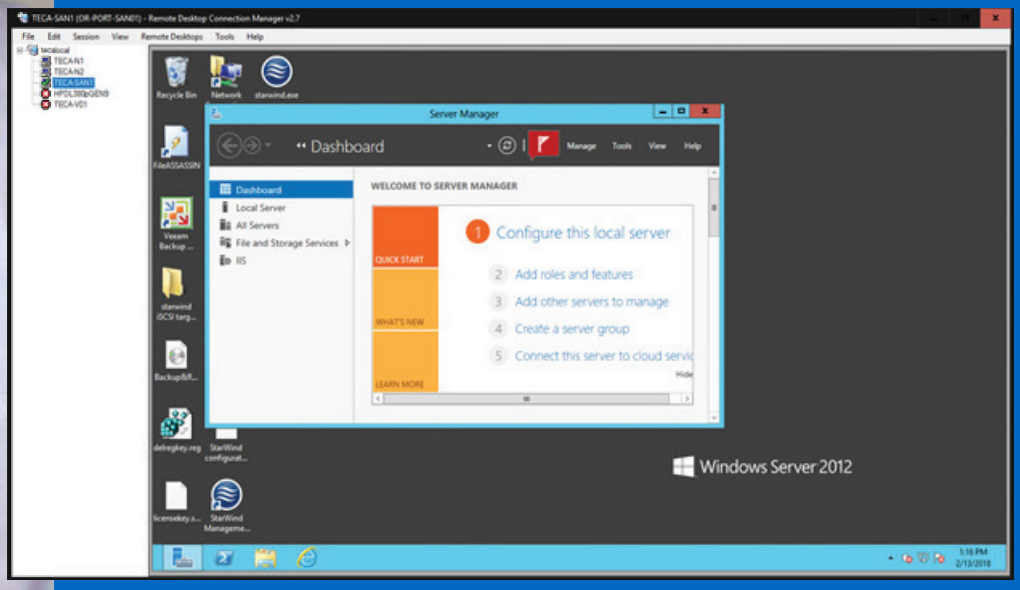


Figure 1 –Remote Desktop Connection Manager de Microsoft

Comme vous pouvez le voir dans la Figure 1, RDCMan vous permet de créer des groupes de différents systèmes distants auxquels vous pouvez vous connecter. Chaque groupe est stocké dans un fichier. rdg distinct qui peut être exporté et partagé par d'autres utilisateurs. Il est important de comprendre qu'il s'agit de documents distincts, ce qui peut compliquer les modifications par lots et leur partage avec plusieurs utilisateurs. RDCMan offre également la possibilité de chiffrer vos identifiants stockés à l'aide de certificats. Les connexions à distance ont la possibilité d'hériter des paramètres du groupe dont elles font partie ou vous pouvez personnaliser chaque session à distance. Par défaut, l'affichage à distance est rendu dans le cadre principal de la console RCDMan, mais vous avez également la possibilité de désancrer la session à distance. RCDMan est avant tout un outil de gestion Windows. Il peut utiliser RDP pour se connecter à des sessions Windows distantes et il peut également se connecter à des sessions de console Hyper-V VM en utilisant VMConnect.

RDCMan fonctionne bien pour la gestion d'un petit nombre de systèmes. Malheureusement, il présente plusieurs limitations lorsqu'il est utilisé dans un contexte d'entreprise – petite ou grande. Voici quelques-unes des principales limitations de RCDMan :

- Pas de prise en charge Linux et Mac - RDCMan est principalement conçu pour utiliser avec Windows et il ne prend pas en charge toute la gamme de serveurs que l'on trouve dans la plupart des entreprises aujourd'hui.
- Pas officiellement soutenu par Microsoft - Une chose importante que beaucoup d'administrateurs ne réalisent pas, c'est que RDCMan n'est pas un produit officiel de Microsoft et qu'il n'est pas soutenu ni mis à jour par Microsoft. La dernière mise à jour de RDCMan date de 2014.
- Saisie manuelle des informations d'identification - RDCMan vous oblige à saisir manuellement les données d'identification pour vos sessions à distance. Ça peut prendre du temps et entraîner des erreurs.
- Bureau à distance uniquement - RDCMan ne fournit pas d'outils ou de capacités de mise en réseau supplémentaires.

Devolutions Remote Desktop Manager

La plupart des entreprises ont des besoins de gestion des connexions à distance qui vont au-delà des capacités de base fournies par l'offre gratuite de Microsoft. Devolutions Remote Desktop Manager (RDM) offre la possibilité de gérer plusieurs connexions de bureau à distance. De plus, RDM offre un ensemble d'outils beaucoup plus complet et des capacités de gestion spécifiquement conçues pour les entreprises, chose que RDCMan n'offre pas. Examinons de plus près quelques-unes des principales fonctionnalités et outils de gestion des connexions à distance de RDM.

Tout d'abord, RDM est pris en charge sur presque toutes les plateformes de bureau et de serveur Windows les plus populaires, notamment : Windows Vista SP2, Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 SP2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2 et Windows Server 2016.

La dernière version requiert également Microsoft .NET Framework 4.6. Il existe des versions 32 bits et 64 bits de RDM.

RDM offre une interface moderne avec un menu à ruban et une interface à onglets pour chaque session à distance ouverte. Vous pouvez voir un aperçu de Devolutions Remote Desktop Manager à la figure 2.

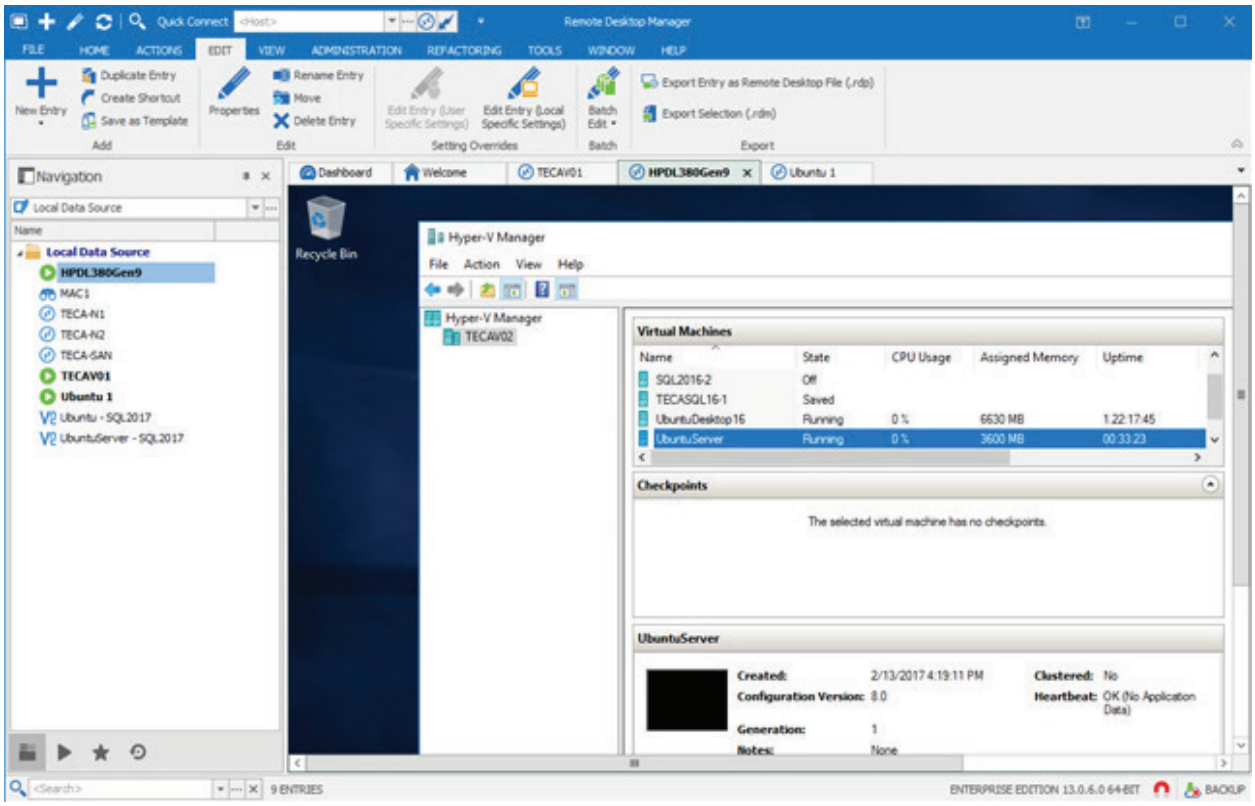


Figure 2 – Devolutions Remote Desktop Manager

RDM est essentiellement divisé en un volet de navigation, que vous pouvez voir sur le côté gauche de la Figure 2, et en une zone contextuelle, que vous pouvez voir sur le côté droit. Le volet de navigation contient des entrées qui peuvent être des sessions de bureau à distance comme dans la Figure 2 ou autres types d'entrées telles que des informations d'identification, des contacts, des documents et des macros/scripts/outils.
Vous pouvez rapidement créer plusieurs entrées en cliquant avec le bouton droit de la souris sur une entrée, puis en sélectionnant Dupliquer l'entrée dans le menu contextuel. Vous pouvez, si vous le souhaitez, modifier l'affichage par défaut du volet de navigation, qui passe de l'arborescence illustrée à la figure 2 à une vue en mosaïque ou à une vue détaillée. Le volet de contenu est utilisé pour afficher différentes sessions de bureau à distance ainsi que les résultats des divers outils et commandes intégrés qui font partie de RDM.

Dans la Figure 2, vous pouvez voir que les entrées des sessions de bureau à distance sont regroupées sous une source de données. Les sources de données définissent l'endroit où les entrées sont stockées et elles peuvent être partagées entre différents utilisateurs. Vous pouvez organiser toutes vos sessions à distance sous les différentes sources de données. Par exemple, vous pouvez avoir une source de données différente ou unité commerciale que vous gérez.

RDM offre un contrôle granulaire sur chaque connexion, chaque groupe de connexions ou chaque source de données. Par défaut, toutes les sessions ouvertes apparaissent dans leurs propres onglets dans la zone contextuelle. Vous pouvez travailler avec chaque source de données et chaque session en cliquant avec le bouton droit de la souris dans le volet de navigation. Si vous utilisez l'affichage par onglets, vous pouvez passer rapidement d'une session à l'autre en cliquant sur l'onglet souhaité. RDM vous offre la possibilité de faire apparaître vos connexions dans une interface à onglets ou comme une connexion de bureau à distance standard. Pour la prise en charge de plusieurs écrans, RDM vous permet de créer une fenêtre conteneur séparée de la fenêtre principale. Vous pouvez faire glisser et déposer les onglets ouverts sur la fenêtre conteneur.

SOURCES DE DONNÉES PARTAGÉES

Presque toutes les entreprises, petites et grandes, comptent plusieurs personnes utilisant des connexions de bureau à distance. Ces utilisateurs sont souvent répartis entre différents sites. Pour faciliter l'accès, les informations de connexion des sessions RDM peuvent être stockées dans un certain nombre de sources de données partagées. Ces sources de données et leurs sessions peuvent être partagées par plusieurs membres de l'équipe. RDM prend en charge les sources de données partagées suivantes :

- **Amazon S3** - Peut être partagé en mode lecture seule. Support de base.
- **Devolutions Online Database** - Support de base pour les microéquipes (jusqu'à 3 utilisateurs), les éditions Professional et Enterprise supportent les plus grandes équipes.
- **Devolutions Server** – Partagé. Prend en charge toutes les fonctionnalités, telles que les pièces jointes, le journal des connexions, le mode hors connexion et la gestion de la sécurité.
- **Dropbox** - Peut être partagé en mode lecture seule.
- **FTP** – Utilise un fichier XML qui peut être partagé en mode lecture seule.
- **Google Drive** - Partagé. Prend en charge toutes les fonctionnalités, telles que les pièces jointes, le journal des connexions, le mode hors connexion et la gestion de la sécurité.
- **MariaDB** - Partagé. Prend en charge toutes les fonctionnalités, telles que les pièces jointes, le journal des connexions, le mode hors connexion et la gestion de la sécurité.
- **Microsoft Access** – Partagé mais non recommandé, parce que Microsoft ne le prend pas en charge dans les versions les plus récentes de Windows.
- **Microsoft SQL Azure** -- Partagé. Prend en charge toutes les fonctionnalités, telles que les pièces jointes, le journal des connexions, le mode hors connexion et la gestion de la sécurité.
- **Microsoft SQL Server** – Partagé. Source de données recommandée pour les utilisateurs multiples. Prend en charge toutes les fonctionnalités, telles que les pièces jointes, le journal des connexions, le mode hors connexion et la gestion de la sécurité.
- **MySQL** - Partagé. Prend en charge toutes les fonctionnalités, telles que les pièces jointes, le journal des connexions, le mode hors connexion et la gestion de la sécurité.
- **SFTP** – Peut être partagé en mode lecture seule. Support de base.
- **SQLLite** - Partagé. Prend en charge toutes les fonctionnalités, telles que les pièces jointes, le journal des connexions, le mode hors connexion et la gestion de la sécurité.
- **WebDav** - Peut être partagé en mode lecture seule. Support de base.

Les sources de données qui sont stockées dans le nuage sont généralement sauvegardées automatiquement par le fournisseur de services infonuagiques. Pour protéger les données sensibles de vos sources de données, vous pouvez verrouiller la configuration de la source de données avant de la déployer. Le mode hors ligne vous permet de vous connecter à une copie locale de la source de données lorsque la base de données active est indisponible. Il peut être utilisé lorsqu'un utilisateur travaille depuis un réseau déconnecté ou en cas de problème de connectivité à la source de données. La fonctionnalité d'édition par lots de RDM vous permet de modifier facilement les paramètres de plusieurs sessions en une seule opération. Par exemple, de nombreuses entreprises ont un cycle de changement de mot de passe de 90 jours, ce qui peut devenir un problème lorsque vous devez changer régulièrement les mots de passe pour plusieurs connexions. RDM vous permet également d'associer des mots-clés/balises à vos entrées, ce qui facilite la recherche d'entrées similaires.

PLUSIEURS TYPES D'HÔTES ET DE CONNEXIONS À DISTANCE

Les infrastructures informatiques d'aujourd'hui sont généralement tout sauf homogènes. Outre la gestion des serveurs Windows, la plupart des entreprises doivent également gérer des serveurs Linux et parfois des systèmes Mac. De plus, les administrateurs ont souvent besoin de se connecter directement à des VM Hyper-V ou VMware ainsi que d'utiliser d'autres services comme FTP ou VPN. Le RDCMan de Microsoft est essentiellement limité à RDP et ne peut pas se connecter à une bonne partie des systèmes que les administrateurs informatiques d'aujourd'hui doivent gérer. Les capacités de connectivité à distance offertes par Devolutions RDM couvrent toute la gamme de connectivité requise par les entreprises. Outre Windows et RDP, RDM prend en charge de multiples protocoles distants comme VNC pour la connectivité Linux, Apple Remote Desktop, Citrix ICA as, Hyper-V et VMware ainsi que d'autres produits de contrôle/gestion à distance comme HP Integrated Lights Out (iLO) et LogMeIn. RDM vous permet de consolider votre gestion des connexions à distance en utilisant un seul outil pour vous connecter à des systèmes distants Windows, Linux, etc. Vous pouvez voir la variété des connexions à distance prises en charge par RDM dans la Figure 3.

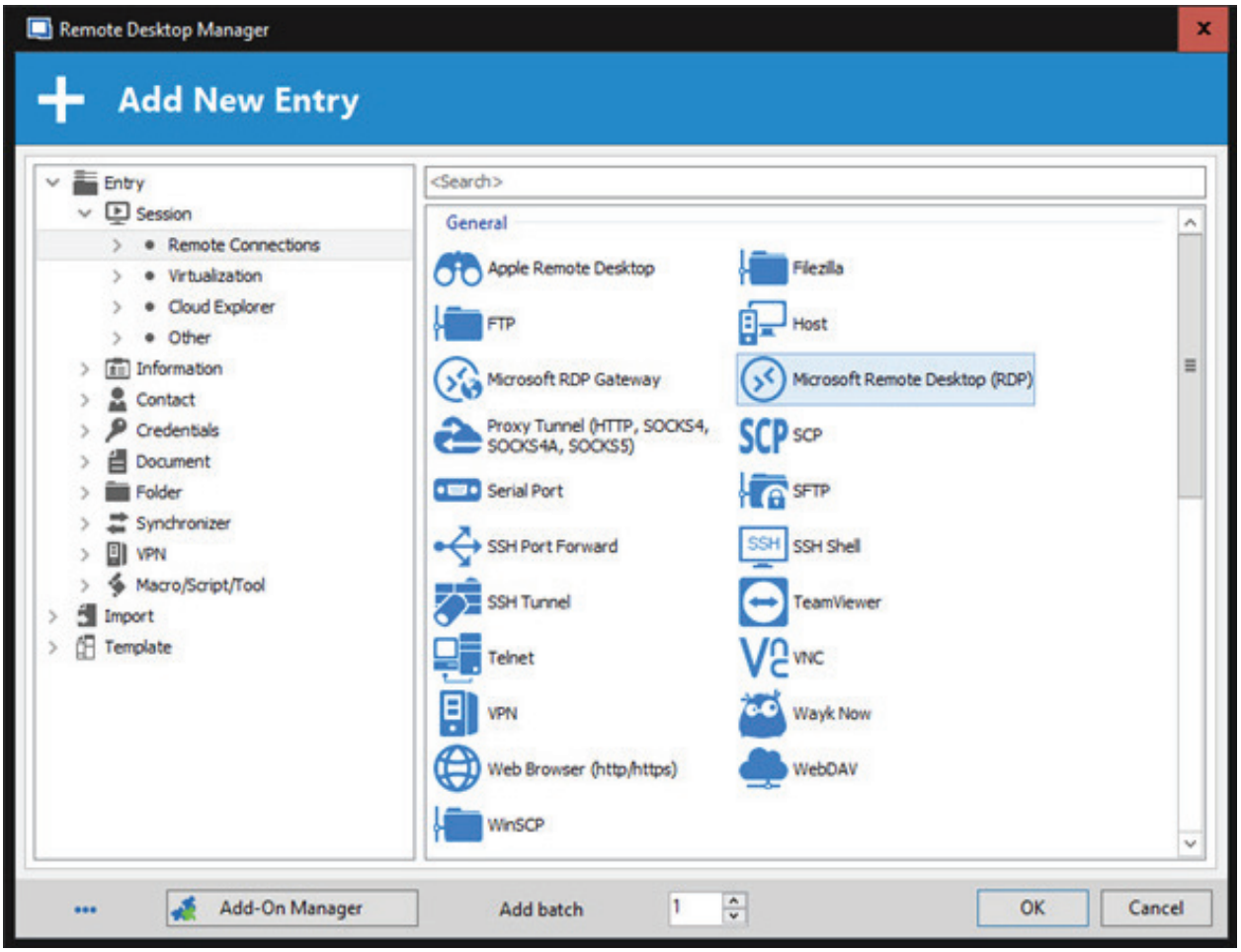


Figure 3 – Remote Desktop Manager supporte ces connexions à distance

Pour créer une nouvelle session à distance, sélectionnez le type de session souhaité, puis RDM vous invite à définir les propriétés de configuration spécifiques à cette session. Comme vous pouvez le voir sur la Figure 3, le large éventail de sessions distantes prises en charge par RDM vous permet de répondre à l'ensemble des besoins de l'entreprise. Voici les types de sessions distantes les plus courantes prises en charge par RDM :

- Microsoft Remote Desktop (RDP) – Pour les connexions aux systèmes Windows
- VNC – Pour les connexions aux systèmes Linux
- Apple Remote Desktop – Pour les connexions aux systèmes Apple
- Telnet – Pour les connexions à divers hôtes Telnet Windows et Linux
- FTP, SFTP, SCP & WinSCP – Pour les connexions aux hôtes FTP

Sécurité de niveau entreprise

Il est essentiel de sécuriser correctement vos connexions de bureau à distance en raison de l'étendue des possibilités d'accès et d'administration qu'elles offrent. RDM fournit plusieurs fonctionnalités de sécurité de niveau de l'entreprise qui peuvent vous permettre de sécuriser l'accès à vos sessions à distance. Les mots de passe constituent la première couche de toute stratégie de sécurité et RDM offre de nombreuses fonctionnalités qui peuvent vous aider à gérer les mots de passe des sessions distantes. RDM permet la gestion centralisée des mots de passe à distance, la génération de mots de passe et l'application des politiques de mots de passe. La centralisation de tous les mots de passe et de toutes les données d'entreprise en un seul endroit sécurisé permet aux administrateurs d'accéder rapidement aux informations dont ils ont besoin et de les conserver en un seul endroit sécurisé. RDM est capable d'appliquer toutes les politiques de mots de passe essentielles pour les sessions à distance, dont :

- Historique des mots de passe – Détermine quand un ancien mot de passe peut être réutilisé.
- Âge du mot de passe – Détermine quand un utilisateur doit changer son mot de passe.
- Longueur minimale du mot de passe – Détermine le nombre minimal de caractères requis pour un mot de passe.
- Exigences de complexité – le mot de passe ne doit pas contenir le nom de l'utilisateur et doit utiliser au moins trois des quatre types de caractères possibles : lettres minuscules, lettres majuscules, chiffres et symboles.

L'analyseur de mots de passe intégré est une autre fonctionnalité de sécurité importante de RDM. Lorsque vous fournissez des mots de passe pour vos sessions à distance, l'analyseur de mots de passe de RDM évalue automatiquement les mots de passe et vous indique s'ils sont forts ou faibles. RDM est également capable de générer automatiquement des mots de passe forts et sécurisés. L'activation de la politique d'audit des mots de passe vous permet de suivre tous les changements de mot de passe.

Pour gérer la sécurité de l'accès à distance des utilisateurs ayant des responsabilités et des besoins d'accès à distance différents, RDM fournit un système de sécurité basé sur les rôles qui permet une protection granulaire flexible. Par exemple, vous pouvez créer des rôles et des paramètres de sécurité différents pour vos administrateurs, l'équipe du soutien TI ou les consultants. La sécurité basée sur les rôles de RDM permet d'hériter des paramètres de sécurité. Les éléments et dossiers enfants sont automatiquement couverts par les paramètres de sécurité d'un dossier parent. Les autorisations spécifiques d'un élément donné peuvent être remplacées. Vous pouvez définir des autorisations pour un sous-dossier ou un élément afin de remplacer les autorisations de l'élément parent.

RDM offre également plusieurs autres fonctionnalités importantes de sécurité par rapport aux accès à distance. Tout d'abord, il dispose d'une fonctionnalité d'enregistrement et de retrait qui permet à un administrateur de verrouiller l'accès à une session à distance. Par exemple, si vous effectuez une maintenance de longue durée et que vous ne souhaitez pas autoriser d'autres personnes à accéder au système, vous pouvez verrouiller la session et les autres utilisateurs ne pourront pas y accéder tant qu'elle n'aura pas été réenregistrée. Vous pouvez également restreindre l'accès aux sessions distantes en fonction du temps.

Par exemple, vous pouvez autoriser l'accès à certaines sessions à distance uniquement pendant les heures de bureau. RDM prend également en charge l'authentification à deux facteurs. Cette fonctionnalité n'est disponible que pour les sources de données suivantes : SQLite, Online Database, Devolutions Server, MariaDB, Microsoft Access, SQL Azure, SQL Server et MySQL.

Les journaux sont une autre fonctionnalité de sécurité importante fournie par RDM. RDM enregistre l'utilisation de toutes vos sessions à distance, dont l'ouverture et la fermeture des sessions, ainsi que leur durée. Ils enregistrent également l'affichage ou la modification des entrées ainsi que l'identité de la personne qui a effectué l'action.

Outils de gestion à distance

Une gestion à distance efficace exige plus qu'une simple connexion interactive au système distant. Dans de nombreux cas, vous devez réparer la connectivité du réseau, vérifier la configuration d'un serveur distant ou effectuer une variété d'autres tâches de gestion et de dépannage. Outre la gestion de bureaux à distance, RDM fournit un certain nombre d'outils pratiques de gestion de réseau que vous pouvez utiliser pour gérer vos systèmes distants. Vous pouvez voir la collection d'outils de gestion de systèmes distants fournis par RDM dans la Figure 4.

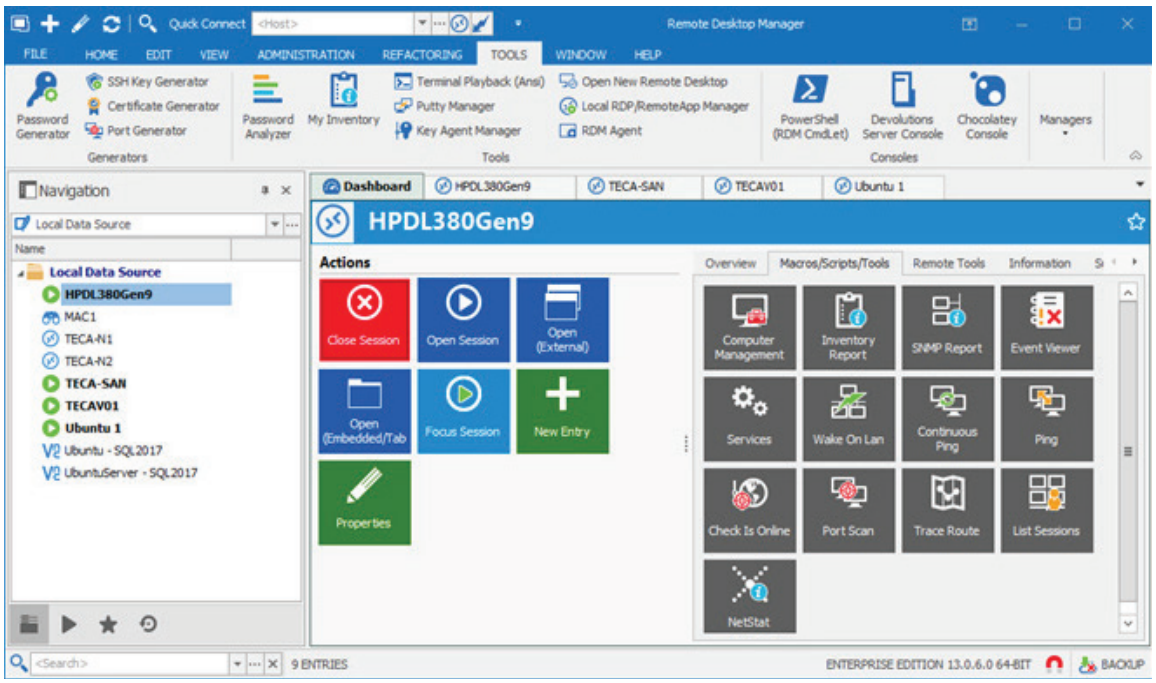


Figure 4- Les outils de gestion à distance de Remote Desktop Manager

Scripts PowerShell

RDM prend également en charge les scripts Windows PowerShell, qui permettent aux administrateurs d'automatiser la gestion de RDM. RDM fournit un module PowerShell appelé RemoteDesktopManager.PowerShellModule.dll qui se trouve dans le répertoire d'installation de Remote Desktop Manager. Vous pouvez utiliser la cmdlet Import-Module pour charger le module dans vos sessions PowerShell. Le module PowerShell RDM peut être utilisé pour automatiser une grande variété de tâches, notamment :

- Se connecter aux sources de données
- Créer des bases de données
- Charger des documents de configuration
- Attribuer des identifiants aux entrées
- Récupérer les propriétés de la session
- Modifier les propriétés des dossiers de groupe et des sessions
- Définir les rôles des clients
- Importer et exporter des CSV

Gestion des connexions à distance de niveau entreprise

La gestion des connexions à distance est l'une des choses les plus importantes utilisées par les administrateurs informatiques d'aujourd'hui. RDM de Devolutions va bien au-delà de la connectivité Windows de base offerte par le RDCMan de Microsoft. RDM offre des fonctionnalités de niveau entreprise comme la connectivité à toutes les plateformes de serveurs populaires, la gestion des groupes, la sécurité et les scripts pour la gestion à distance. RDM vous permet de centraliser toutes vos connexions à distance, vos identifiants et vos outils dans une seule plateforme qui peut être partagée en toute sécurité par vos administrateurs et les autres utilisateurs du bureau à distance.

COMMANDITÉ PAR DEVOLUTIONS

Devolutions