Briefing du webinaire Petri
5 octobre 2018

PME : La sécurité des Bureaux à distance

Présentateur : Michael Otey
Modérateur : Brad Sams, Petri IT Knowledgebase, Éditeur principal pour petri.com

Il ne fait aucun doute que les outils de bureaux à distance facilitent le travail des administrateurs système de PME. Ces solutions sont particulièrement utiles pour l'administration à distance, parce qu'elles permettent d'avoir une session interactive avec vos systèmes distants. L'administrateur peut ainsi travailler exactement comme s'il était au bureau. Il n'est pas nécessaire d'apprendre d'autres outils de gestion à distance qui peuvent être difficiles à configurer et à utiliser ou des technologies de script compliquées.

Le Bureau à distance permet aux administrateurs de diagnostiquer et de résoudre les problèmes... à distance. Cependant, il s'agit d'un outil puissant qui utilise souvent un accès hautement privilégié aux systèmes distants de votre réseau. La sécurité y est donc d'une importance capitale. Le *Federal Bureau of Investigation* (FBI) et le *Department of Homeland Security* (DHS) recommandent aux entreprises d'examiner et de comprendre leur utilisation du Bureau à distance et de prendre des mesures pour réduire la probabilité de compromission. Ils soulignent que l'absence de mesures de sécurité appropriées peut ouvrir la porte à des attaques de logiciels malveillants et de rançongiciels. Ces attaques peuvent être difficiles à repérer, parce qu'elles ne nécessitent aucune intervention de l'utilisateur. Voyons de plus près ce qu'est RDP et ce que sont les principaux problèmes de sécurité que l'administrateur réseau doit connaître en matière de Bureau à distance.

Comprendre le protocole RDP

Pour sécuriser correctement le Bureau à distance, il est important de comprendre comment il fonctionne. Il utilise le protocole propriétaire de Microsoft, Remote Desktop Protocol (RDP), pour se connecter à des systèmes distants.

Par défaut, RDP utilise le port TCP 3389 et le port UDP 3389. RDP est conçu pour prendre en charge différents types de topologies réseau et plusieurs protocoles LAN. Sur le serveur cible, RDP a son propre pilote vidéo qui sert à envoyer la sortie d'affichage dans les paquets réseau au client du Bureau à distance.

Le client RDP reçoit les données d'affichage et les convertit en appels d'API d'interface de périphérique graphique (GDI) de Microsoft Windows.

Les activités liées à la souris et au clavier sont redirigées du client vers le serveur. Le serveur RDP utilise son propre pilote de clavier et de souris pour traiter ces activités. En outre, RDP a la capacité de rediriger d'autres ressources locales du client vers la cible RDP distante, notamment le presse-papiers, les imprimantes et les lecteurs locaux.

Les risques liés à RDP

Le Bureau à distance est un outil puissant et il existe un certain nombre de risques de sécurité liés à RDP, surtout si vos serveurs de Bureau à distance sont accessibles depuis l'Internet. Un balayage à l'échelle de l'Internet effectué par des chercheurs en sécurité de Rapid7 a montré qu'il y avait plus de 11 millions d'appareils avec des ports 3389/TCP laissés ouverts en ligne. Ce chiffre est en hausse par rapport au début de l'année 2016, lorsqu'une analyse précédente avait trouvé 9 millions d'appareils avec le port 3389 ouvert. De nombreuses entreprises, en particulier les PME, ne sont pas conscientes des risques liés à l'exposition potentielle du protocole RDP sur Internet.

RDP peut être une cible de piratage attrayante, parce que la sécurité est généralement liée à un domaine Active Directory (AD) pour l'authentification. Si AD ou ses domaines de confiance sont mal configurés, les pirates peuvent obtenir des informations d'identification de vos ressources internes privées.

Par exemple, même si vous utilisez un domaine DMZ pour les bureaux à distance, une mauvaise configuration de vos domaines d'entreprise peut entraîner des failles de sécurité.

RDP est un vecteur de sécurité important. Si les pirates trouvent un moyen d'accéder à RDP, ils peuvent valider les comptes d'utilisateurs, exposer les mots de passe et infecter vos systèmes internes avec des logiciels malveillants et des rançongiciels.

Attaque par force brute
L'une des attaques les plus courantes contre les systèmes RDP exposés est le piratage des mots de passe par force brute. Lors de ces attaques, le pirate dispose généralement d'une petite liste d'identifiants et utilise ensuite un logiciel de piratage automatisé pour générer rapidement un grand nombre de mots de passe.

En juillet 2018, LabCorp, l'un des plus grands laboratoires cliniques des États-Unis, a été victime d'une attaque par force brute contre RDP. Le tout a été orchestré par le groupe Samsam. Ce dernier a obtenu l'accès via RDP et a pu déployer un rançongiciel sur le réseau de LabCorp. Bien que l'attaque n'ait pas abouti à une violation des données, elle a pu chiffrer des milliers de systèmes et des centaines de serveurs de production ont été mis hors ligne pendant la restauration des systèmes.

Il s'agissait essentiellement du même rançongiciel qui avait été utilisé pour attaquer la Ville d'Atlanta en 2017. Se protéger contre les attaques par force brute est vital pour tout système RDP.

Pulvérisation de mots de passe
Une autre méthode d'attaque RDP courante est connue sous le nom de pulvérisation de mots de passe (de l'anglais *password spraying*).

Avec ce type d'attaque, il y a généralement une longue liste de noms d'utilisateurs et une petite liste de mots de passe choisis stratégiquement qui sont utilisés pour tenter de se connecter aux différents comptes d'un même domaine.

La pulvérisation de mots de passe permet aux pirates de tenter de nombreuses connexions sans bloquer les utilisateurs, parce qu'elle évite les tentatives de connexion répétées avec le même identifiant. Cette technique peut être efficace, surtout lorsqu'on sait que de nombreux employés utilisent des mots de passe faibles.

La liste des comptes susceptibles d'être attaqués est souvent établie par les pirates en exploitant des sources d'information accessibles au public comme Google, LinkedIn et Facebook.

Attaque de l'homme du milieu
Les anciennes versions de RDP et les mauvaises configurations peuvent également exposer une entreprise à des attaques de type « homme du milieu ». Essentiellement, une attaque de ce type peut faire en sorte que le trafic RDP passe par un hôte différent de celui prévu par l'utilisateur. Cet hôte intermédiaire est alors en mesure de visualiser le trafic réseau RDP et, dans certains cas, de le manipuler, voire de modifier le niveau de sécurité négocié entre le serveur et le client. Le nom et le mot de passe de l'utilisateur peuvent ainsi être capturés, ce qui entraine alors d'autres problèmes de sécurité potentiels.

Sécuriser RDP

Il existe différentes options pour les PME qui souhaitent sécuriser leurs connexions de Bureau à distance. L'utilisation de toutes (ou d'une partie) de ces options peut contribuer à protéger l'infrastructure informatique.

La sécurité commence par la garantie que tous vos utilisateurs utilisent des mots de passe forts. Les mots de passe forts qui ne peuvent pas être facilement devinés offrent une protection de base pour les données sensibles de votre organisation. Ils ajoutent aussi une couche de protection contre les attaques par force brute et par pulvérisation de mots de passe. Des outils comme Remote Desktop Manager (RDM) de Devolutions peuvent garantir que les mots de passe de votre bureau à distance sont forts. Comment? En s'assurant que les politiques de mots de passe soient respectées, notamment par rapport à la longueur, le niveau de complexité et la (non) réutilisation des mots de passe.

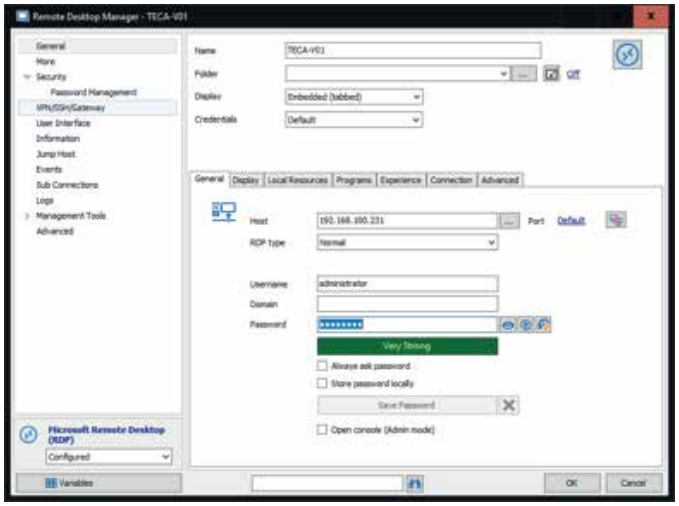

Figure 1 – Utiliser des mots de passe forts avec Remote Desktop Manager

RDM fournit également une jauge utile de la force du mot de passe lorsque vous créez une nouvelle session RDP. Vous pouvez voir la qualité du mot de passe de RDM dans la Figure 1.

Verrouillage de comptes RDP avec des stratégies de sécurité

Changer les utilisateurs par défaut qui sont autorisés à utiliser les services de Bureau à distance peut également améliorer la sécurité de votre RDP.

Figure 2 – Verrouillage des utilisateurs RDP
Vous pouvez éventuellement supprimer les deux groupes répertoriés par défaut dans « Autoriser la connexion » via les propriétés du bureau à distance, puis sélectionner « Ajouter un utilisateur ou un groupe » pour ajouter les utilisateurs ou les groupes que vous souhaitez voir explicitement autorisés à utiliser les services de bureau à distance.

Par défaut, les stratégies de sécurité locales de Windows permettent au groupe Administrateur et au groupe Utilisateurs du Bureau à distance de se connecter.

Si vous voulez changer ça, vous pouvez ouvrir *Local Security Policy* en utilisant le gestionnaire de serveur. Sélectionnez *Tools and Local Security Policy* ou entrez la commande secpol.msc. Dans la boîte de dialogue *Local Security Policy*, développez le sous-menu *Local Policies*, puis *User Rights Assignment*. Double-cliquez ensuite sur l'option *Allow log on* via les services Bureau à distance. La boîte de dialogue illustrée à la Figure 2 s'affiche alors.

Utilisation des stratégies de verrouillage des comptes

Les stratégies de verrouillage des comptes peuvent également contribuer à renforcer la sécurité de votre Bureau à distance.

Elles peuvent empêcher les pirates et autres personnes non autorisées de deviner vos mots de passe manuellement ou à l'aide d'outils automatiques. Les stratégies de verrouillage de compte empêchent l'utilisation de la session RDP pendant une période donnée après un certain nombre de tentatives de connexion échouées. Vous pouvez configurer une stratégie de verrouillage de compte en utilisant le gestionnaire de serveur, en sélectionnant *Tools*, puis *Local Security Policy* ou avec la commande secpol.msc. Développez le sous-menu *Account Policies* et sélectionnez ensuite *Account Lockout Policies* comme vous pouvez le voir sur la Figure 3.

Vous pouvez alors définir le temps pendant lequel un compte sera verrouillé. Bien que la durée spécifique du verrouillage dépende des besoins de l'entreprise, il est généralement recommandé de commencer par trois minutes. Le seuil de verrouillage du compte indique le nombre d'échecs de connexion qui entraînera le verrouillage du compte d'un utilisateur. En général, il est recommandé de le fixer entre 4 et 10. Pour l'option « réinitialiser le compteur de verrouillage du compte après », il est recommandé que cette valeur soit inférieure ou égale à la durée de verrouillage du compte.

Chiffrement des connexions RDP

Beaucoup de PME partent du principe selon lequel RDP est toujours sécurisé par le chiffrement le plus élevé disponible par défaut. Cependant, les connexions client RDP négocient en fait avec l'hôte le niveau de chiffrement qui sera utilisé. RDP utilise RC4 de RSA Security qui est conçu pour chiffrer efficacement de petites quantités de données pour des communications sécurisées sur les réseaux. Les administrateurs peuvent choisir de chiffrer les données en utilisant une clé de 56 ou 128 bits.

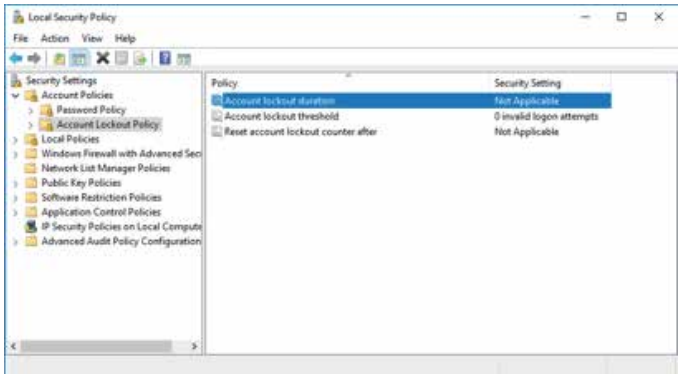

Figure 3 – Définir les stratégies de verrouillage de comptes

Pour définir le niveau de chiffrement RDP sur le système cible RDP de Windows Server 2016, vous pouvez lancer Local Group Policy Editor à partir du gestionnaire de serveur ou avec la commande gpedit.msc. À partir de l'éditeur, développez Computer Configuration, puis Administrative Templates, Windows Components, Remote Desktop Services, Remote Desktop Session Host, puis cliquez sur Security. Les stratégies de sécurité RDP du serveur s'affichent alors, comme le montre la Figure 4. Pour vous assurer que les sessions RDP sur ce système sont chiffrées aux niveaux les plus élevés, sélectionnez Set client connection encryption level policy. La boîte de dialogue illustrée à la Figure 5 s'affiche.

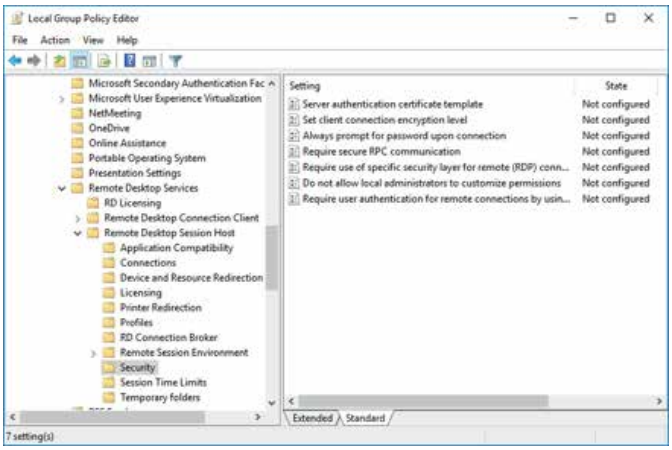

Figure 4 – Définir les politiques de sécurité RDP de l'hôte de Windows Server 2016

Pour vous assurer que les sessions RDP sur ce système sont chiffrées aux niveaux les plus élevés, sélectionnez Set client connection encryption level policy. La boîte de dialogue illustrée à la Figure 5 s'affiche.

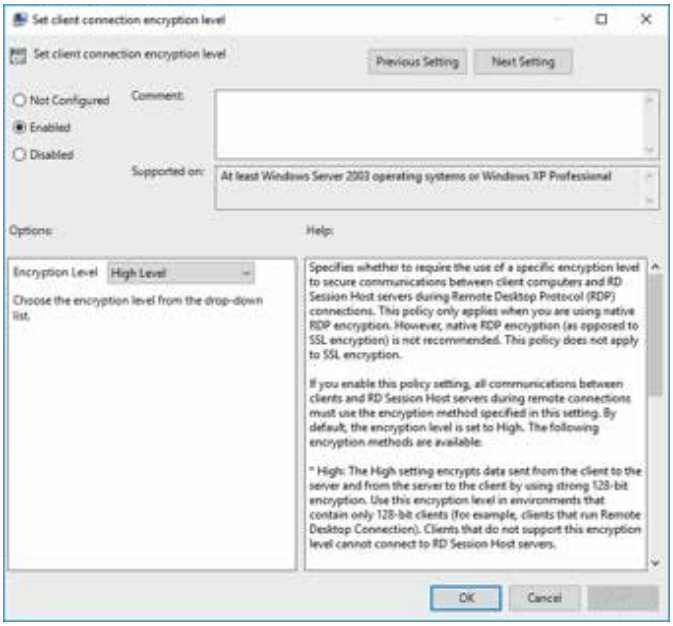

Figure 5 - Définir le niveau de chiffrement de la connexion client

Pour définir le niveau de chiffrement, cliquez sur le bouton radio Enabled en haut de la boîte de dialogue, puis utilisez la liste déroulante Encryption Level pour sélectionner le niveau élevé. Ainsi, les sessions de Bureau à distance seront sécurisées par un chiffrement de 128 bits.

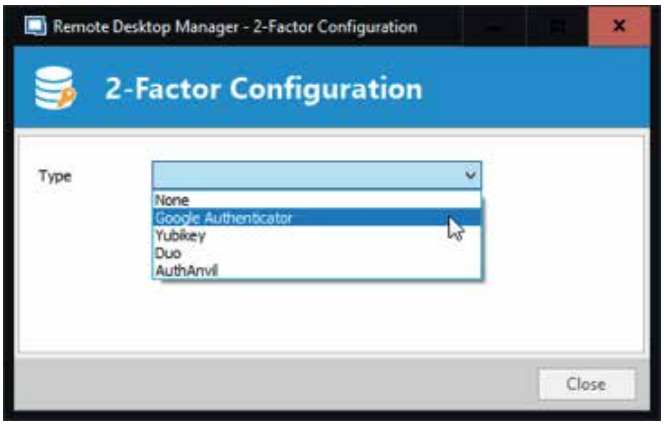

Figure 6 – Configuration de l'authentification à deux facteurs avec RDM

Utiliser l'authentification à deux facteurs

L'authentification à deux facteurs (A2F) est un autre outil qui peut vous aider à sécuriser les connexions RDP. Elle permet de renforcer la sécurité lors de l'identification de l'utilisateur en combinant deux composants de connexion différents. Ces composants sont généralement quelque chose que l'utilisateur connaît, comme un mot de passe, et quelque chose que l'utilisateur possède, comme une clé ou une carte à puce.

L'authentification à deux facteurs offre un niveau de sécurité plus élevé, puisqu'il est moins probable qu'un utilisateur non autorisé soit capable de fournir les deux facteurs d'authentification requis. Pour utiliser cette stratégie avec RDP, vous devez généralement intégrer des produits tiers.

Les sources de données de Remote Desktop Manager prennent en charge plusieurs options d'authentification à deux facteurs, notamment Duo, Google Authenticator, Yubikey et AuthAnvil.

Il est important de ne pas faire l'erreur de penser que l'A2F est à elle seule une solution complète pour la sécurité de RDP. Pour être vraiment efficace, elle doit être appliquée uniformément dans toute l'organisation.

Par exemple, si vous disposez d'un VPN utilisant l'authentification à deux facteurs, mais que d'autres services derrière le VPN ne disposent pas du A2F, un pirate peut les exploiter pour accéder à votre infrastructure. Pour une protection maximale, l'authentification à deux facteurs doit être configurée pour tous les actifs exposés qui ont accès à des informations sensibles. La figure 6 présente un exemple de son utilisation avec RDM.

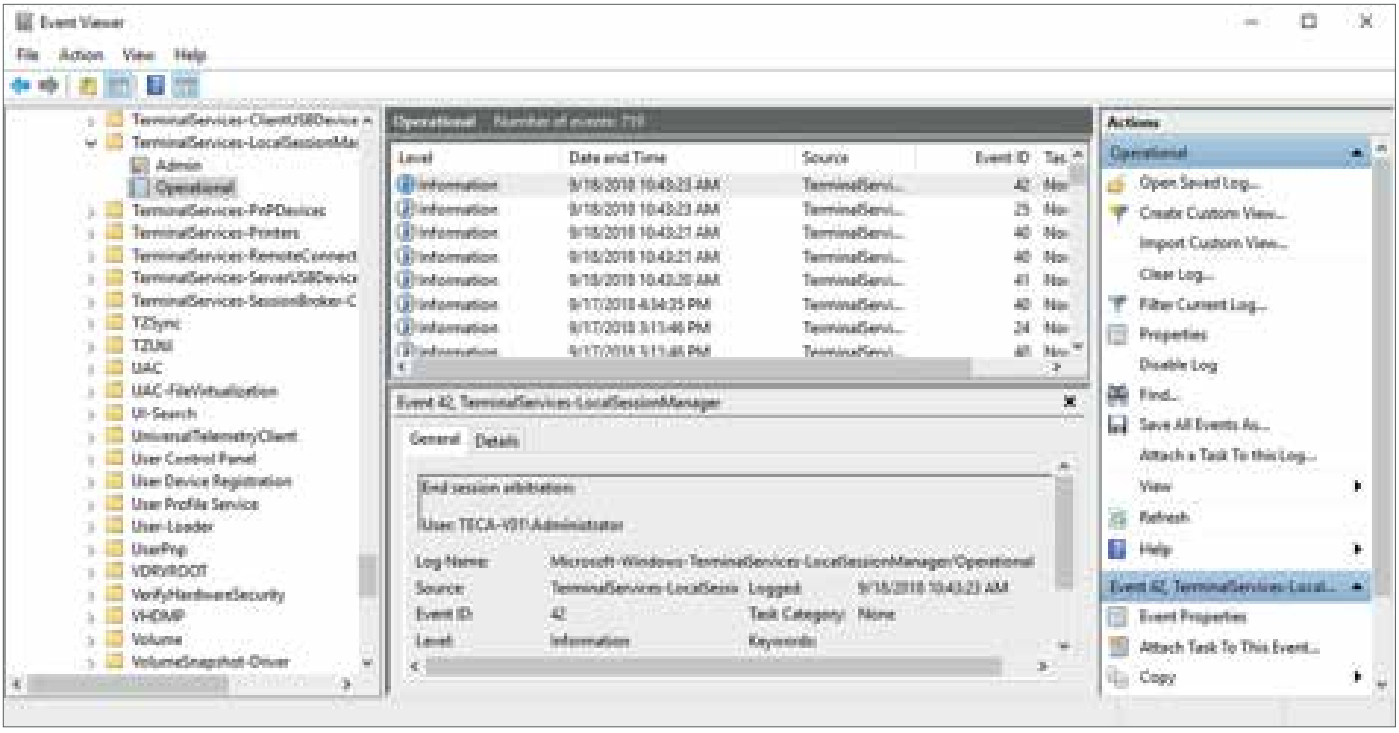

Figure 6 - Utilisation du journal d'activité du Bureau à distance

Suivi de l'activité des connexions à distance

La surveillance régulière de l'activité de votre Bureau à distance est un autre facteur important pour assurer la sécurité de votre infrastructure informatique. Une surveillance régulière peut vous aider à détecter si des tentatives de connexion non autorisées échouent régulièrement.

Vous pouvez utiliser l'Observateur d'événements de Windows Server pour suivre l'activité de connexion au Bureau à distance en allant dans le gestionnaire de serveur, puis en sélectionnant *Tools* et *Event Viewer*. Développez le sous-menu *Applications and Services logs*, puis *Microsoft*, *Windows*, *TerminalServices-LocalSession-Manager*. Finalement, sélectionnez *Operational*. L'utilisation d'un système de gestion centralisée comme RDM de Devolutions peut offrir des informations sur l'activité du Bureau à distance avec un niveau de détail nettement supérieur. Comme vous pouvez le voir à la Figure 7, le journal d'activité de RDM fournit une vue consolidée et centralisée de toute l'activité du Bureau à distance de votre organisation. RDM suit le système de connexion, la date, l'heure, l'utilisateur et l'ordinateur pour toutes les sessions RDP.

En outre, RDM peut également assurer la gestion et le suivi de la grande majorité des connexions à distance utilisées par la plupart des entreprises, notamment les connexions VNC, FTP, Telnet, SSH, VPN et par navigateur Web.

Protéger RDP à l'aide d'une stratégie de défense en profondeur

Sécuriser RDP pour les PME est tout aussi important que pour les grandes entreprises – peut-être même plus, parce que les failles de sécurité pour les PME peuvent avoir un impact global plus important sur l'entreprise. La défense en profondeur est donc la meilleure approche. En plus de sécuriser RDP à l'aide des stratégies décrites dans ce document, il est vital que vous mainteniez vos systèmes d'exploitation client et serveur à jour. Les services critiques doivent se trouver derrière un VPN et ne pas être directement exposés sur Internet. Les VPN sont conçus pour séparer et sécuriser vos ressources privées contre les attaques extérieures. Ils sont renforcés et conçus pour interdire tout accès non autorisé à vos systèmes et services (comme RDP). Même si le VPN est attaqué, le pirate n'aura pas accès à votre infrastructure d'entreprise.

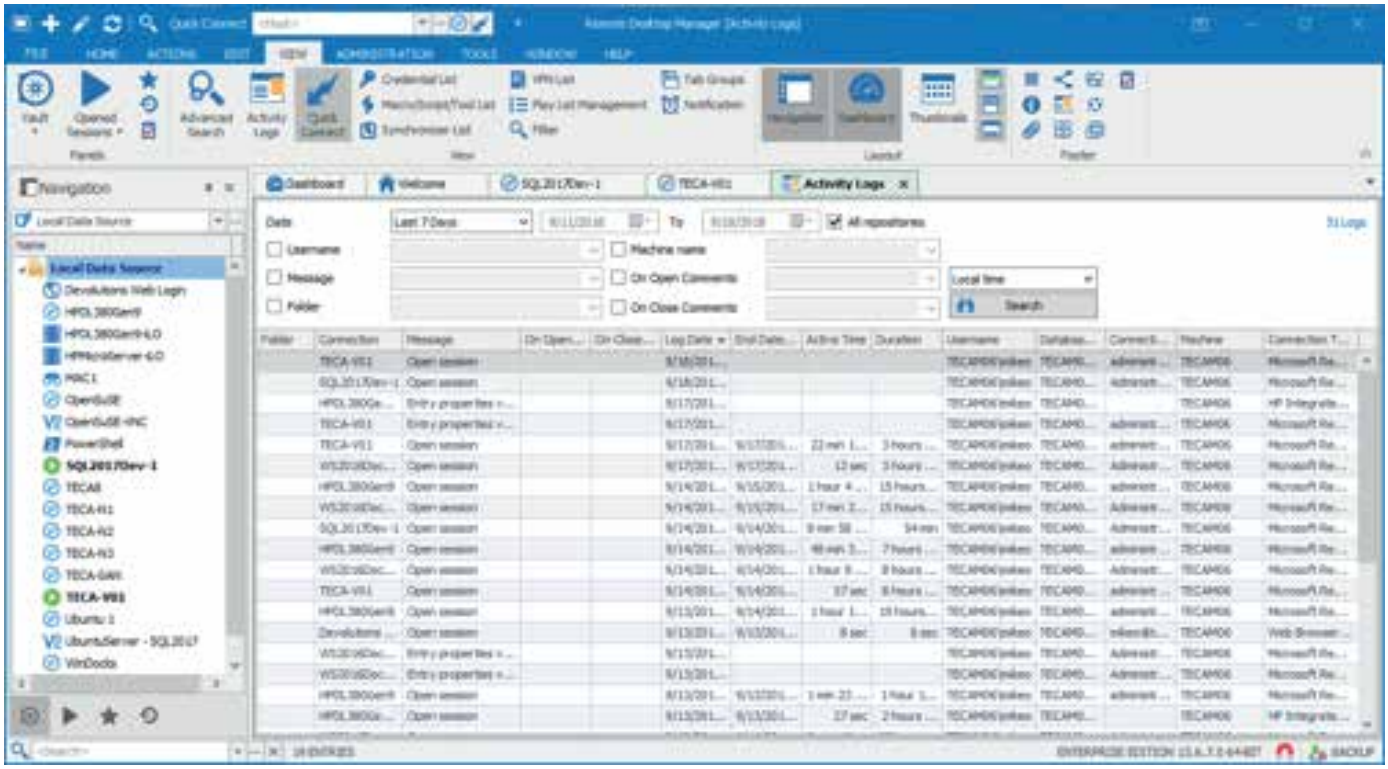

Figure 7 - Suivi de l'utilisation du Bureau à distance avec le journal d'activité de RDM