Top 5 des fonctionnalités à rechercher dans une solution de gestion des connexions à distance

DOCUMENT TECHNIQUE

TABLE DES MATIÈRES

Comment la gestion des connexions à distance peut faciliter le travail des administrateurs système

Les administrateurs système sont prêts pour une révolution dans leur façon de faire leur travail. Lors d'une journée typique, ils se connectent à des systèmes distants en utilisant le protocole RDP (Remote Desktop Protocol), PuTTY, des outils basés sur un navigateur, des logiciels propriétaires, des réseaux privés virtuels (VPN) et autres technologies de connexion à distance. Ces outils sont indispensables: personne ne veut revenir à l'époque où l'on essayait de régler un problème en parlant aux utilisateurs par téléphone.

Sauf que ces mêmes outils peuvent aussi nuire à la productivité. Les administrateurs système utilisent en effet plusieurs technologies de connexion à distance qui prennent en charge des protocoles spécifiques et qui ont leurs propres outils et interfaces utilisateur. Pour ajouter à la complexité de leur travail, les administrateurs système ont souvent des dizaines, voire des centaines, d'ensembles d'informations d'identification à stocker et à protéger. Certains ont recours à des méthodes peu sûres de gestion des mots de passe, comme l'utilisation de feuilles de calcul et de texte en clair dans des documents de script. Bien sûr, certains gèrent l'accès des utilisateurs par l'intermédiaire de Microsoft Active Directory, mais les utilisateurs doivent alors saisir leurs informations d'identification des dizaines de fois dans la journée. Ces réalités sont contreproductives et rendent le travail des administrateurs système plus difficile.

Une solution de gestion des connexions à distance qui répond à ces défis peut vraiment changer la donne, surtout si elle possède les cinq fonctionnalités essentielles décrites dans ce document.

Devolutions Remote Desktop Manager

TechTarget Custom Media

LES PRINCIPALES FONCTIONNALITÉS D'UNE BONNE SOLUTION DE GESTION DES CONNEXIONS À DISTANCE

Si vous voulez que votre solution de gestion des connexions à distance aide les administrateurs système à faire leur travail, elle devrait offrir ces cinq principales fonctionnalités :

1. Gérer un large éventail de technologies et de protocoles de connexion à distances.
2. Stocker les mots de passe des comptes et autres informations sensibles dans un coffre sécurisé.
3. Partager en toute sécurité les paramètres de session entre les utilisateurs.
4. Gérer les rôles, les autorisations et les droits de sécurité des utilisateurs.
5. Organiser et récupérer facilement les sessions grâce à une interface utilisateur intuitive.

FONCTIONNALITÉ 1 : GÉRER UN LARGE ÉVENTAIL DE TECHNOLOGIES ET DE PROTOCOLES DE CONNEXION À DISTANCE

Chaque jour, les écrans des administrateurs système sont remplis de fenêtres. Ils doivent parfois utiliser SSH, FTP, Telnet, RDP, VNC, HTTPS, TeamViewer, LogMeIn et bien d'autres outils pour accéder à des ordinateurs distants. Et ça, c'est juste avant le déjeuner! Chaque outil a sa propre interface, ses coûts de licence et ses exigences. Ce grand nombre de protocoles et d'outils ajoute de la complexité au travail et peut nuire à la productivité, parce que les administrateurs système doivent jongler avec les différentes fenêtres pour passer d'une session distante à l'autre.

Une solution idéale devrait prendre en charge, à un seul endroit, tous les protocoles et outils avec lesquels les administrateurs système travaillent, y compris les VPN. Cette solution remplacerait de nombreuses fenêtres ouvertes par une seule interface qui contiendrait toutes les sessions, ce qui éviterait d'avoir à passer d'une session à l'autre et de se retrouver avec des barres de tâches surchargées.

FONCTIONNALITÉ 2 : STOCKER LES MOTS DE PASSE DES COMPTES, LES INFORMATIONS D'IDENTIFICATION ET AUTRES INFORMATIONS SENSIBLES DANS UN COFFRE SÉCURISÉ

Les administrateurs système ont souvent des dizaines, voire des centaines de mots de passe à gérer, sans parler des numéros de compte, des cartes de crédit, des clés de licence de logiciels et de plusieurs autres informations. Souvent, ces données sensibles sont stockées dans différents endroits, comme des applications de gestion des mots de passe, des sessions RDP enregistrées et même des feuilles de calcul, ce qui rend difficile le suivi des bonnes pratiques en matière de sécurité et de conformité.

Une solution complète de gestion des connexions à distance devrait permettre aux administrateurs système d'accéder à ces informations de n'importe où et de remplir automatiquement les formulaires de connexion. En outre, les administrateurs système qui utilisent une application de gestion des informations d'identification comme KeePass devront s'assurer que la solution de gestion des connexions à distance s'intègre à leur application de gestion des informations d'identification ou permet au moins de l'exploiter.

Une solution qui offre un coffre sécurisé renforce la sécurité et favorise la conformité, parce que les informations sont stockées dans une base de données centralisée protégée par le chiffrement AES (pour Advanced Encryption Standard). Elle simplifie également le travail des administrateurs système en éliminant les multiples emplacements pour stocker les données dont ils ont besoin pour faire leur travail.

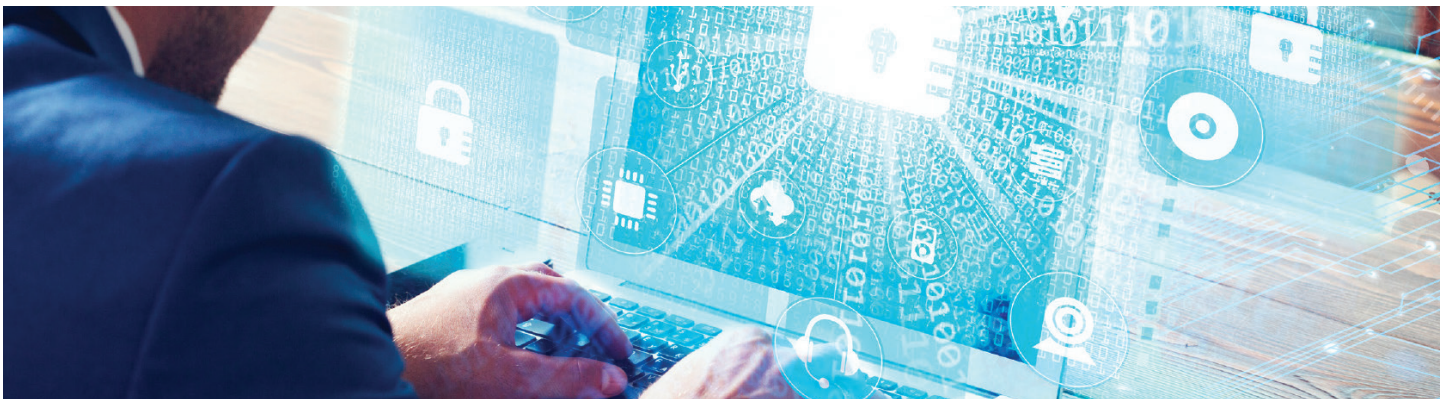
FONCTIONNALITÉ 3 : PARTAGER EN TOUTE SÉCURITÉ LES PARAMÈTRES DE SESSION ENTRE LES UTILISATEURS

Lorsqu'un administrateur système fait face à un problème de gestion de connexions à distance, il peut être utile de partager la session avec un collègue. Sauf que le faire de manière sécuritaire et efficace est tout un défi. Les administrateurs système ont souvent recours au partage des paramètres de connexion et des informations d'identification par des moyens longs et peu sécurisés, comme par courriel, via les applications de messagerie instantanée ou en les notant sur un papier. Cette approche nuit à la productivité, à la sécurité et à la conformité.

Une bonne solution de gestion des connexions à distance devrait stocker les paramètres de connexion et les informations d'identification dans une base de données centralisée et chiffrée afin que les utilisateurs n'aient pas à partager manuellement des informations sensibles. Ainsi, les membres de l'équipe qui ont les autorisations appropriées peuvent accéder à la même session. Le système peut même afficher ou masquer certaines informations en fonction des droits des utilisateurs. Ces fonctionnalités permettent de gagner du temps et peuvent renforcer la sécurité et la conformité.

FONCTIONNALITÉ 4 : GÉRER LES RÔLES, LES AUTORISATIONS ET LES DROITS DE SÉCURITÉ DES UTILISATEURS

Le contrôle d'accès basé sur les rôles est essentiel dans les environnements d'équipe. Sans lui, les administrateurs ont du mal à faire respecter la séparation des tâches et les autres contrôles qui visent à garantir que les membres de l'équipe ne voient que ce qu'ils ont le droit de voir, et rien d'autre. Pour renforcer la sécurité et la conformité, les administrateurs système doivent pouvoir gérer les rôles, les autorisations et les droits des utilisateurs de manière à ce que ces derniers n'aient accès qu'aux informations d'identification et aux connexions auxquelles ils sont autorisés.



La bonne solution doit permettre aux administrateurs de gérer facilement l'accès en définissant des droits spécifiques pour un ou plusieurs utilisateurs. Recherchez une solution qui permet un contrôle granulaire par la création de rôles et de groupes avec des autorisations spécifiques pour accéder aux sessions.

La solution doit pouvoir s'intégrer aux outils de contrôle d'accès des utilisateurs existants comme Active Directory. Les changements aux groupes Active Directory (ajout de nouveaux utilisateurs ou modification des rôles) devraient être automatiquement partagés à la solution de gestion des connexions à distance.

Une autre fonctionnalité importante dans un environnement multiutilisateur est la surveillance et le suivi. La solution doit avoir des fonctionnalités de journalisation complètes pour que les organisations puissent suivre qui a ouvert, fermé ou modifié des sessions.

FONCTIONNALITÉ 5 : ORGANISER ET RÉCUPÉRER FACILEMENT LES SESSIONS GRÂCE À UNE INTERFACE UTILISATEUR INTUITIVE

Les administrateurs système ont des centaines de connexions à gérer. Des fonctionnalités puissantes et une interface utilisateur intuitive peuvent donc faire la différence entre productivité et frustration.

La solution devrait permettre aux administrateurs système d'organiser facilement les connexions à distance de manière intuitive. Par exemple, ils pourraient vouloir créer un dossier pour les connexions de l'organisation aux serveurs en nuage et un autre pour les connexions sur site.

Une solution puissante offrira aux administrateurs système de multiples options de visualisation grâce à une structure de liste arborescente. La solution devrait également leur permettre d'épingler les sessions auxquelles ils accèdent le plus souvent et inclure une fonction de recherche afin qu'ils puissent retrouver les sessions plus rapidement.

Finalement, la solution devrait fournir des gabarits qui permettent aux administrateurs système de gagner du temps lors de la création de connexions.

LAISSEZ LA GESTION DE CONNEXIONS À DISTANCE CHANGER VOTRE TRAVAIL AU QUOTIDIEN

Une solution de gestion des connexions à distance qui offre les cinq fonctionnalités décrites ici peut transformer (pour le mieux) le travail des administrateurs système. Remote Desktop Manager de Devolutions offre ces fonctionnalités et plus encore. Il prend en charge plus de 60 modules complémentaires et les administrateurs système peuvent le personnaliser pour qu'il fonctionne avec les technologies existantes de l'organisation - des VPN aux outils de gestion des mots de passe en passant par les clients de connexion à distance.

Remote Desktop Manager a aidé les administrateurs système de milliers d'entreprises à transformer leur façon de travailler. Selon Eric Olmstead, programmeur senior en automatisation des versions chez Siemens Building Technologies :

« L'un des grands avantages est que nous pouvons désormais gérer en toute sécurité nos connexions et nos informations d'identification. C'est facile de les protéger, de les mettre à jour et de les partager. C'est aussi tellement facile d'autoriser l'accès, pour un nouveau technicien, à un certain nombre de connexions et/ou d'informations d'identification, simplement en le plaçant correctement dans les groupes AD. Il n'est plus nécessaire d'envoyer des connexions par courriel ou de les stocker dans un emplacement du réseau, ni d'envoyer des informations d'identification par SMS, etc. »

Plus de 300 000 utilisateurs dans le monde profitent d'avantages similaires avec Remote Desktop Manager. Vous êtes prêt à le voir en action? Contactez Devolutions pour une démonstration en direct à : **https://remotedesktopmanager.com/fr/home/requestdemo.**