3 facteurs qui contribuent au chaos informatique quand les employés travaillent à distance

Comment la gestion des connexions à distance aide les administrateurs système à offrir un service efficace et sécurisé aux utilisateurs

Table des matières

Le sort des administrateurs système dépend beaucoup des connexions à distance, notamment quand vient le temps d'aider rapidement les utilisateurs à résoudre leurs problèmes, où qu'ils soient dans le monde.

Pris individuellement, les mécanismes de gestion de services Bureau à distance semblent assez simples. Pour une seule session, il suffit d'utiliser le bon protocole et d'avoir accès aux informations d'identification appropriées pour établir une connexion et accéder au système. Sauf qu'en réalité, les administrateurs système doivent s'adapter aux différents types de ressources informatiques, aux divers protocoles de connexion, aux nombreux utilisateurs et aux différents groupes d'entreprises ou environnements clients. La difficulté de gérer de manière sécurisée les informations d'identification et de configurer les connexions pour chaque situation commence à peser lourd.

Si les équipes informatiques gèrent manuellement les connexions, le nombre de mots de passe et de paramètres de configuration va rapidement entraîner le chaos. Et les problèmes surgissent généralement sur trois fronts.

TechTarget | Custom Media

Devolutions

Remote Desktop Manager

Facteur 1 : La fragmentation, ça complique les choses

Chaque système utilisateur a ses propres exigences de configuration basées sur les politiques réseau, les outils d'accès à distance, les protocoles et les informations d'identification. À grande échelle, c'est très difficile pour les équipes de TI de gérer et de partager toutes ces informations de connexion et d'identification. Idéalement, lorsque les administrateurs TI doivent accomplir une tâche, ils devraient pouvoir accéder rapidement et sans effort à chaque système concerné. Toutefois, actuellement, de nombreuses organisations s'appuient sur un mélange complexe de feuilles de calcul Excel et de documents Word pour garder une trace des informations de connexion pertinentes.

Avec des approches manuelles comme celles-ci, les administrateurs ont du mal à faire un bon suivi des nouvelles machines et à garder à jour les informations de serveur, de connexion et d'identification. Ça veut dire que chaque fois qu'ils jouent dans un nouveau système à distance, les administrateurs système doivent chercher les informations à gauche et à droite. Résultat? C'est plus long et plus difficile de se connecter.

Facteur 2 : Une mauvaise gestion des utilisateurs augmente les risques

Non seulement les suivis manuels complexifient le travail de l'administrateur système, mais ils entraînent également de nombreux risques. L'absence de contrôles automatisés sur les mots de passe, les informations d'identification et les privilèges ajoute un risque inutile au processus de connexion à distance.

D'un point de vue réglementaire et de gestion des risques, les équipes TI ont besoin d'un moyen de donner accès sans jamais exposer les informations d'identification des utilisateurs pendant le processus. Aussi, les entreprises doivent gérer les privilèges pour que chaque administrateur système ne puisse pas nécessairement accéder à tous les systèmes. Ça nécessite des contrôles de sécurité qui peuvent limiter les privilèges d'un groupe d'administrateurs système en fonction de la sensibilité du système en question.

Un processus manuel ne permet pas de gérer les risques sur plusieurs systèmes ou bases de clients. En plus, la configuration de sessions sur une base ad hoc empêche la reproductibilité dans les normes de configuration. Il y a donc plus de chances d'avoir de mauvaises configurations qui pourraient potentiellement être exploitées par des pirates informatiques.

Facteur 3 : Les configurations manuelles, c'est contre-productif

La complexité d'avoir à gérer manuellement de nombreuses variables de connexion a des répercussions sur le nombre d'heures de travail des administrateurs système. Surtout s'ils doivent établir des connexions à distance à plusieurs reprises tout au long de la journée.

S'ils doivent entrer une adresse IP, récupérer des paramètres de connexion, démarrer une instance de Remote Desktop Protocol ou configurer une session à chaque fois qu'ils travaillent sur une nouvelle tâche, ils vont rapidement perdre le contrôle sur leur quotidien. Ça représente une énorme perte de productivité qui peut, en fin de compte, avoir un impact sur les résultats du département.

Contrôlez le chaos avec Remote Desktop Manager

Les équipes informatiques doivent contrôler le chaos informatique. Elles ont besoin d'un système pour centraliser les informations de configuration/connexion et pour gérer les informations d'identification des utilisateurs sans exposer les mots de passe. Elles doivent éviter d'avoir à faire une tonne de tâches administratives juste pour établir une connexion.

Les administrateurs ont besoin d'une solution capable de s'adapter à des centaines de types de connexion, avec une interopérabilité à grande échelle et qui ne favorise pas une technologie en particulier. Et ils ont besoin d'une piste d'audit claire pour prouver la sécurité des connexions aux clients et aux organismes de contrôle et de réglementation.

Devolutions Remote Desktop Manager (RDM) fait tout ça. C'est un système facile d'utilisation et efficace qui enregistre les connexions à distance, les mots de passe et les documents connexes sur une seule plateforme sécurisée.

En centralisant les données, c'est beaucoup plus facile d'ajouter, modifier, supprimer, partager, organiser et chercher des connexions et des informations d'identification à distance.

RDM dispose d'une interface intuitive qui agit comme un couteau suisse pour gérer les accès à distance. Cette solution offre plus de 160 technologies et protocoles intégrés, y compris des modules complémentaires qui prennent en charge plus de 25 types de réseaux privés virtuels (RPV).

Plus important encore, la connectivité est gérée de manière sécurisée. Les équipes TI peuvent facilement intégrer leurs gestionnaires de mots de passe existants directement dans RDM. La plateforme est conçue de manière à ce que les administrateurs système n'aient jamais accès directement aux informations d'identification des utilisateurs. Aussi, les privilèges sont gérés par des permissions et par des groupes pour plus de flexibilité. Ça permet faire une séparation des tâches pour protéger les données sensibles et respecter les réglementations en matière de sécurité des données.

Devolutions aide ses clients à vaincre ces trois facteurs

Devolutions aide les organisations à contrôler le chaos informatique engendré par ces trois facteurs. Voici comment RDM a aidé les experts TI chez GolfNow, Siemens Building Technologies et EchoStar :

Sur la complexité : « Je me connecte en moyenne à 20 ou 30 machines par jour. Si je devais chaque fois chercher l'adresse du serveur, mes informations d'identification, mes informations RPV, ouvrir le RPV, ouvrir la machine et taper mes informations d'identification, je ne serais pas capable de fonctionner ou d'atteindre la même productivité. » – Justin Azevedo, responsable des services de données chez GolfNow

Sur la sécurité : « Un des grands avantages, c'est que nous pouvons désormais gérer nos connexions et nos informations d'identification en toute sécurité. Nous pouvons les mettre à jour, les partager et les protéger facilement. C'est aussi extrêmement facile d'ajouter l'accès d'un nouveau technicien à un certain nombre de connexions et/ou d'informations d'identification, simplement en le plaçant correctement dans les groupes AD. Plus besoin d'envoyer des connexions par courriel ou de les stocker dans un emplacement réseau et plus besoin d'envoyer des informations d'identification par SMS. » – Eric Olmstead, programmeur senior en automatisation de versions, Siemens Building Technologies

Sur la productivité : « Au cours de mes 20 ans d'expérience en tant qu'administrateur, j'ai travaillé sur plusieurs types d'interfaces matérielles de réseau et systèmes d'exploitation. Ils sont tous accessibles via un outil différent. Mais avec RDM, je peux faire mon travail en utilisant un seul outil! RDM est vraiment une console unique pour tous mes besoins d'administration à distance. » – David Sechler, spécialiste du personnel, systèmes/réseaux, EchoStar

Pour en savoir plus sur Devolutions Remote Desktop Manager et sur la façon dont cette solution peut aider votre entreprise à accroître sa productivité et la sécurité de ses utilisateurs, consultez le https://remotedesktopmanager.com/fr.