Raritan
Know more. Manage smarter.™

Les Entreprises Multisites:
Accès et Gestion de l'Infrastructure Informatique

Vue d'Ensemble

Bien que la prolifération des sites distants et succursales soit un signe positif de la croissance d'une compagnie, cette situation peut constituer un défi pour le personnel informatique. En plus de la gestion des centres de données, les équipes informatiques ont la responsabilité supplémentaire de gérer et de réparer les ressources des bureaux distants tels que les routeurs, les commutateurs, les pare-feu, les optimiseurs de performances des réseaux étendus et les serveurs. Les employés qui travaillent sur les sites distants n'ont généralement pas les connaissances informatiques nécessaires pour résoudre les problèmes. Pour relever ce défi, un grand nombre de responsables informatiques utilisent des solutions logicielles d'accès à distance pour diagnostiquer et réparer les problèmes des bureaux distants. Néanmoins, ces outils sont utiles uniquement si le système d'exploitation et le réseau fonctionnent. Si le réseau ou le système d'exploitation est en panne, il peut être demandé à un employé sur le site d'accéder à l'armoire serveur pour tenter de résoudre le problème. Si cela ne marche pas, des coûts supplémentaires en temps, déplacement et manque à gagner peuvent être encourus.

Ce livre examine la valeur ajoutée (en termes de disponibilité et de sécurité) des outils d'accès et de gestion hors bande pour les bureaux distants.

Défis des bureaux distants

Il est estimé, selon le Groupe Internet Research, que rien qu'aux Etats-Unis il y a plus de 1.5 millions de filiales en communication directe avec leur siège. Et cette estimation ne prend pas en compte les services de kiosques, ATM et autres sites de transactions en libre service.

En élargissant la portée des entreprises, les bureaux distants alourdissent également la tâche des responsables informatiques, chargés de l'installation, la surveillance et la maintenance des ressources informatiques des divers emplacements distants. Ces ressources peuvent inclure les dispositifs réseau, tels que les routeurs, les commutateurs, les optimiseurs de performances des réseaux étendus et les pare-feu. Elles peuvent également inclure les serveurs d'applications distribuées et de stockage pour les transactions et le courrier électronique.

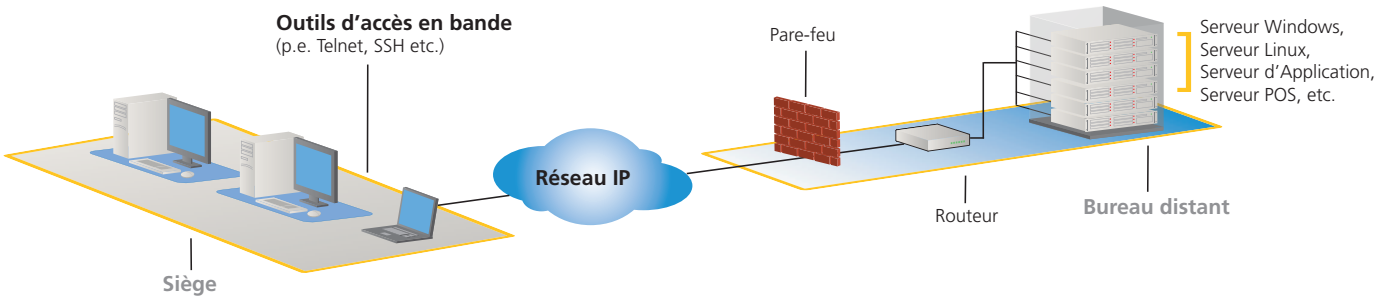
Les défis liés à la gestion des bureaux distants se rangent dans les catégories suivantes :

Contrôle et complexité : Les réseaux de bureaux distants peuvent comporter un ensemble de composants hétérogènes en termes de dispositifs et de fabricants. La complexité croissante de ces réseaux rend plus difficiles la gestion et la réparation des défaillances. Dans un même temps, lorsque des centaines, voire des milliers de ressources informatiques sont dispersées dans le monde entier, un tableau de bord centralisé pour la gestion des dispositifs devient essentiel.

Sécurité : Un grand nombre de bureaux distants, en particulier les magasins et les banques, possèdent des informations sur les clients sensibles et/ou des données de carte de crédit vulnérables aux intrusions s'ils ne disposent pas de solutions de sécurité appropriées. La prolifération de la technologie Wi-Fi dans les sites complique encore davantage la question de la sécurité.

Budgets et ressources limités : généralement, les bureaux distants n'ont pas de personnel informatique sur le site. Dans ce type de scénario répandu, il revient aux administrateurs informatiques du siège social de diagnostiquer et réparer les problèmes de réseaux et de serveurs. Ceci implique parfois de se déplacer jusqu'au bureau distant pour le dépannage, ce qui peut augmenter la durée moyenne des réparations ainsi que les coûts liés au déplacement. Une autre possibilité consiste à faire se déplacer un fournisseur de services sur le site, ce qui peut également s'avérer onéreux.

Si le problème est critique et doit être corrigé dans l'immédiat, le déplacement n'est pas toujours une solution adéquate. Les outils d'accès à distance deviennent le moyen idéal de se connecter et de corriger les problèmes informatiques à l'intérieur aux bureaux distants et sites distants. La plupart des solutions d'accès à distance se répartissent en catégories en bande et hors bande.



Options d'accès en bande

Logiciels de gestion à distance : ce type de solution permet aux administrateurs informatiques d'accéder au bureau et aux applications exécutés sur les serveurs cibles. Un inconvénient majeur des logiciels de gestion à distance est le fait qu'ils nécessitent la disponibilité du système d'exploitation. Si le système d'exploitation est gelé ou se plante, il n'est plus possible d'accéder au serveur. Par ailleurs, ces solutions logicielles sont tributaires d'une connexion à la carte d'interface réseau du serveur cible. Si le réseau n'est pas disponible, il n'est plus possible de réparer le problème.

Le tableau 1 illustre l'écart entre le logiciel d'accès à distance et les options hors bande telles que KVM sur IP.

	En bande	Hors bande
Tâches	**Logiciel d'accès à distance**	**KVM-sur-IP**
Accès distant aux serveurs	✓	✓
Accès au niveau BIOS	✗	✓
Accès par modem si le réseau est indisponible	✗	✓
Profils utilisateur, autorisations d'accès aux ports	✗	✓
Prise en charge d'utilisateurs multiples, sessions simultanées	✗	✓
Redémarrage à chaud	✓	✓
Redémarrage à froid	✗	✓*
Journalisation	✗	✓

*Utilisation avec une gestion de l'alimentation à distance

Tableau 1

Protocoles d'émulation de terminal : Telnet et son équivalent chiffré SSH sont utilisés pour accéder à et configurer les dispositifs avec ports série : routeurs, commutateurs, pare-feu, unités de distribution d'alimentation et serveurs. Tout comme le logiciel de gestion à distance, cette méthode d'accès est tributaire de la connexion réseau. Si un problème se pose au niveau du réseau étendu, il peut être nécessaire qu'un responsable informatique se déplace jusqu'au bureau distant pour effectuer les réparations. En outre, ces interfaces de maintenance peuvent rendre les succursales plus vulnérables aux intrusions du réseau étant donné que les pirates peuvent utiliser les mêmes interfaces pour voler des données et introduire des virus.

Les avantages du point de vue de la sécurité d'une solution hors bande telle qu'un serveur de console sécurisée sont présentés dans le tableau 2.

	En bande		Hors bande
Tâches	**Telnet**	**SSH**	**Serveur de console**
Sécuriser les dispositifs	✗	✗	✓
Accès par modem si le réseau est indisponible	✗	✗	✓
Chiffrement	✗	✓	✓
Personnaliser les ports TCP	✗	✗	✓
Mot de passe sécurisé	✗	✗	✓
Verrouillage lors d'une nouvelle tentative de saisie du mot de	✗	✗	✓
SYSLOG	✓	✓	✓
Journalisation des frappes	✗	✗	✓
Bannière d'identification de sécurité	✗	✗	✓

Tableau 2

Options hors bande

Serveurs de console sécurisée : le dénominateur commun de la plupart des déploiements informatiques des bureaux distants est la connectivité réseau, qui nécessite généralement un routeur, un commutateur et un pare-feu. Si ces composants sont défaillants dans un emplacement distant, l'entreprise peut être affectée. La majorité des équipements réseau ont des interfaces série et, comme indiqué plus haut, des outils en bande tels que SSH et Telnet sont des méthodes courantes d'accès et de maintenance. Malheureusement, lorsqu'un problème de réseau se présente, ces outils d'accès deviennent inutilisables. Les serveurs de console sécurisée fournissent un accès distant aux serveurs gérés en série et autres dispositifs série via SSH/Telnet et un navigateur Web. Les serveurs de console sécurisée ont l'avantage de fournir un point d'accès et de contrôle aux serveurs gérés en série, à l'équipement de réseau étendu, aux dispositifs réseau et de gestion de l'alimentation. Un autre avantage est le fait qu'ils peuvent fournir un accès à distance si le réseau étendu n'est pas disponible, permettant d'éviter un déplacement sur l'emplacement distant et de réduire le délai de réparation.

Possibilités suivantes avec un serveur console :

- Droits et authentification
  - Comptes locaux
  - Accès au niveau du port
  - Mots de passe sécurisés
  - Prise en charge Active Directory, LDAP, RADIUS, TACACS+
- Fonctions de la console
  - Journalisation
  - Traps SNMP
  - Blocage de touches Solaris
  - Accès partagé
- Fonctions de gestion
  - Alertes électroniques
  - Prise en charge SNMP
- Méthodes d'accès
  - SSH
  - Telnet
  - Interface Web
  - Option d'appels entrants
- Gestion des installations
  - Double alimentation
  - Gestion de l'alimentation
  - Câblage Cat5

"Une fois, nous avons fait une erreur et entraîné le blocage de notre pare-feu. Nous ne pouvions plus nous connecter au réseau. Nous avons fini par devoir envoyer quelqu'un sur le site, afin d'accéder au serveur pour le redémarrer. Si nous avions eu Dominion® SX à l'époque, le problème aurait été résolu en cinq minutes. C'est sans doute cet incident qui nous a obligé à ajouter une solution de serveur de console série sécurisée Raritan à notre infrastructure informatique."

Kevin Byrne
Ingénieur d'Exploitation Réseau,
Charter Communications

KVM-sur-IP: Les commutateurs KVM permettent d'accéder aux serveurs possédant une interface clavier/vidéo/souris et de les gérer. Ils simulent une situation à l'intérieur du centre de données et un accès direct au serveur.

Les commutateurs KVM sur IP offrent la même expérience, via une connexion IP sécurisée. Un autre avantage de taille est la possibilité d'accéder aux serveurs à partir de n'importe quel emplacement, idéal pour l'accès et la gestion des serveurs de bureaux distants. Qu'ils se trouvent au siège social ou à leur domicile en pleine nuit par tempête de neige, les administrateurs informatiques ont toujours accès aux ressources des bureaux distants.

De plus, les commutateurs KVM sur IP offrent un accès en bande et hors bande. En d'autres termes, les responsables informatiques peuvent accéder à leurs serveurs et les gérer au niveau du système d'exploitation/des applications ou au niveau BIOS si le système d'exploitation ne répond pas. Pour encore plus de sérénité, les commutateurs KVM sur IP avec modems intégrés fournissent une connexion d'accès à distance comme autre méthode d'accès en cas de panne du réseau.

Des fonctions à valeur ajoutée supplémentaires telles que Virtual Media permettent aux responsables informatiques de transférer les fichiers à partir de leur bureau, CR-ROM ou clé USB vers des serveurs du monde entier. Ceci constitue un outil idéal pour mettre à niveau et corriger des sites distants.

Le guide d'achat des solutions KVM sur IP détaille les points à prendre en compte lors de l'acquisition d'un commutateur :

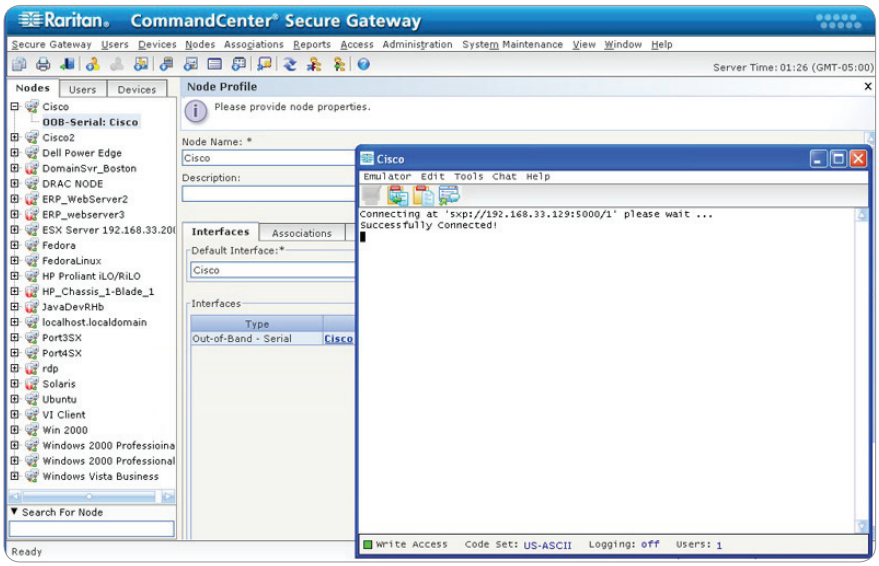
- Accès n'importe où, n'importe quand réel des ressources
  - Prise en charge multiplate-forme
  - Compatibilité bureau/navigateur
  - Accès IP et à distance
  - Client téléchargeable sans frais
  - Accès non bloqué via les ports locaux
  - Gestion complète de remote power control
  - Accès Virtual Media
- Niveau de sécurité et performances
  - Vulnérabilité réduite
  - Contrôles des accès externes et internes
  - Prise en charge Syslog
  - Chiffrement des données
  - Prise en charge des mots de passe sécurisés
- Solutions basées sur un appareil
  - Simplicité de mise en oeuvre
  - Taille et densité des ports
  - Fiabilité et disponibilité

Unités de distribution d'alimentation intelligente : il arrive qu'un redémarrage à froid soit nécessaire comme dernier recours pour résoudre un problème. Bien que les unités de distribution d'alimentation (PDU) soient généralement associées au redémarrage à distance, certaines comportent une intelligence offrant des fonctions de surveillance supplémentaires. Dans une succursale, où l'équipement informatique se trouve généralement dans une armoire ou une petite salle, il est important d'être averti lorsque des facteurs d'environnement et l'usage des ressources d'alimentation dépassent les seuils définis par l'utilisateur. Par exemple, les armoires électriques des petits bureaux ont souvent des systèmes d'aération et de refroidissement médiocres et peuvent n'avoir qu'un seul circuit électrique partagé avec d'autres équipements. Le contrôle de la température de l'armoire et de la consommation des équipements informatiques peut prévenir une panne réseau ou l'endommagement de l'équipement.

Lors de l'acquisition d'une solution de gestion d'alimentation à distance, prenez en compte les fonctions suivantes :

- Accès TCP/IP et série distant à la commutation au niveau des prises
- Délais au niveau des prises, qui peuvent être configurés par l'utilisateur, pour l'alimentation par séquence
- Informations relatives à la surveillance et à l'usage de l'alimentation au niveau de l'unité et au niveau des prises
- Seuils définis par l'utilisateur
- Alertes via SNMP, courrier électronique et Syslog lorsque les seuils sont dépassés
- Prise en charge du chiffrement AES jusqu'à 256 bits et des mots de passe sécurisés
- Prise en charge des options d'authentification et d'autorisation avancées, incluant les autorisations auniveau des prises et LDAP/S, RADIUS et Active Directory®
- Prise en charge des protocoles HTTP, HTTPS, IPMI, SMASH-CLP, SSH, Telnet et SNMP

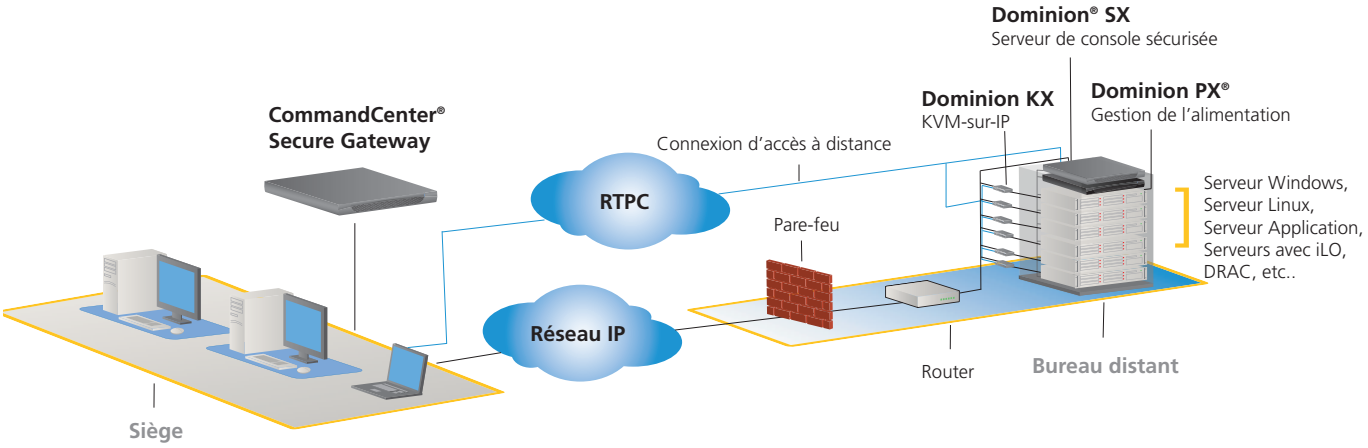
Gestion centralisée : la gestion de dizaines, de centaines voire de milliers d'emplacements peut constituer une tâche laborieuse. Même en disposant de solutions KVM sur IP, serveurs de console sécurisée, Embedded Service Processors (iLO, DRAC, RSA) et PDU intelligentes pour relever les défis liés au dépannage à distance, il est essentiel de pouvoir suivre l'intégralité des ressources hétérogènes dans une vue d'ensemble. Considérez une solution de gestion centralisée capable de prendre en charge une grande variété de dispositifs, ainsi que des fonctions de sécurité et d'autorisation avancées.



Exemple d'écran de CommandCenter® Secure Gateway, qui fournit un accès et une gestion centralisés des dispositifs informatiques.

Conclusion

Bien que rien ne remplace la présence d'un professionnel de l'informatique dans chaque succursale pour veiller au bon fonctionnement des ressources, c'est un luxe que peu d'entreprises peuvent se permettre. La meilleure alternative consiste à disposer des bons outils qui étendent la portée du personnel informatique du siège social aux emplacements distants. Alors que des outils sont actuellement disponibles à coût moindre voire inexistant, le coût en termes de perte de disponibilité et de sécurité est réel. Ceci peut entraîner des dépenses de déplacement et des pannes inattendues, choses que les solutions d'accès à distance sont censées éviter. La meilleure façon de combler les lacunes laissées par les outils d'accès en bande est d'utiliser des solutions hors bande. Pour plus informations sur la manière dont Raritan peut vous aider à gérer et entretenir vos réseaux de bureaux distants, consultez le site **Raritan.fr/branch-office-management**



Engagement de Raritan

Raritan est depuis très longtemps un leader de l'industrie en proposant des produits hautes-technologies pour la gestion des datacenters. L'offre Raritan inclut le Paragon et Dominion - accès sécurisé hors bande et contrôle des serveurs; la famille PX et ses PDU intelligents ; le logiciel de gestion de l'alimentation et de l'énergie du datacenter Power IQ; et maintenant dcTrack -un DCIM avancé, totalement fonctionnel sur les changements et la gestion de capacité du datacenter avec une optimisation des meilleures pratiques pour les charges de travail. Les produits Raritan ont toujours été considérés comme faciles d'utilisation et les plus aboutis. Dès que votre société commence à explorer les outils DCIM, nous vous invitons à considérer dcTrack de Raritan comme votre solution. Basée à Somerset, New Jersey. Raritan possède 38 bureaux dans le monde entier et dessert 76 pays. Pour plus d'informations, visitez le site **Raritan.fr**

C1016 R1