SAN et sécurité. *(Delbrassine Charles)*

Lorsqu'une nouvelle technologie commence à être communément déployée apparaissent souvent les questions de sécurité. Il n'en est pas autrement pour les réseaux de stockage (SAN – Storage Area Network).

Selon une étude « InfoWorld Networked Storage 2002 » il apparaît que 18% des responsables informatiques n'ont pas déployé de réseau de stockage pour des raisons de sécurité et que 56 % des sociétés ayant déployé un SAN planifient sa sécurisation pour l'année en cours.

Lorsque les réseaux de stockage sont apparus sur le marché informatique, la sécurité ne semblait pas un point crucial. Une des raisons était certainement l'utilisation du protocole « Fiber Channel » très peu connu mais aussi simplement parce que la sécurité n'était pas la priorité sur ce type de projets.
De plus il ne faut pas oublier qu'à l'origine le SAN n'était pas conçu pour traverser le globe sur une architecture distribuée, ce sont les utilisateurs qui ont poussé dans cette direction. La combinaison entre l'explosion des volumes stockés, la criticité des données et l'utilisation d'un protocole vulnérable tel qu'IP n'a pas manqué d'attirer l'attention des « hackers ».

Même si la technologie est relativement récente, les principes communs de sécurité restent applicables. Premièrement le réseau de stockage doit être physiquement sécurisé. Ce point est ordinairement couvert car ces architectures ont été déployées dans des salles informatiques existantes. Il y a toutefois lieu d'appliquer les mêmes règles pour tous les sites abritant un élément du réseau (baie de stockage, commutateur, …)

Un des problèmes les plus critiques demeure la facilité de « sniffer » les communications basées sur le protocole « IP ». En 2002, l'IESG (Internet Engineering Steering Group) a publié un décret concernant la sécurité des éléments de stockage et composants réseau. Il impose l'intégration d'une authentification et d'un cryptage à vitesse filaire de type IPSec. En résumé, tout produit de stockage, appareil de contrôle ou adaptateur de bus ainsi que les logiciels associés devront intégrer un système de sécurité compatible IPSec.

Un autre aspect critique demeure le contrôle d'accès aux ressources du réseau de stockage. A l'origine la gestion de l'authentification et des accès n'était pas assez détaillée et n'offrait pas la granularité nécessaire. La plupart des mécanismes en place consistaient simplement à poser cette gestion au niveau des applications et non pas au niveau du composant de stockage lui-même. Face à la problématique de la gestion des accès aux données, la solution la plus communément employée est le « Zoning » et comparable aux « VLANs » utilisés en réseautique. Ces zones peuvent comprendre uniquement certains systèmes de stockage, serveurs ou postes de travail au sein d'une fabrique – restreignant alors l'accès aux seuls équipements « Membres » de la zone définie. Certains fabricants de commutateurs offrent des fonctionnalités propriétaires afin d'augmenter la granularité et de permettre le support d'architecture à haute disponibilité mais aucun standard n'est défini à ce niveau. Même si cette technologie offre une sécurité supplémentaire, elle ne permet nullement de valider si la requête d'un serveur est légitime.

La sécurité globale du réseau de stockage dépend de la sécurité des serveurs et stations accédant aux données ou aux équipements. Il ne faut pas que la prise de contrôle d'un serveur par un utilisateur mal-intentionné soit gérée comme une requête d'accès normale. Face à ce problème, la plupart des fabricants implémentent des contrôles globaux offrant un haut niveau de granularité et qui requièrent une identification de l'utilisateur des données avant tout accès. La gageure est d'arriver à combiner les technologies propriétaires afin de conserver une latitude suffisante au niveau du choix des fournisseurs de solutions.

A ces problèmes, il y a lieu d'ajouter les risques liés au protocole « IP » tels que la prise de contrôle d'équipements visant au déni et à la rupture de service. Cet aspect est à prendre en compte, même sur des architectures locales, car les logiciels de gestion utilisent le protocole « IP » et sont donc autant de passerelles pour attaquer un SAN. La problématique « IP » du SAN est à considérer globalement dans la politique de sécurité couvrant le réseau.

L'analyse de la sécurité du SAN, lors de la mise en place ou de l'audit doit absolument couvrir les domaines suivants :
- *"Administrator to Security Management"* – Domaine entre les administrateurs et leurs applications de gestion.
- *"Host to Switch"* – Domaine entre les serveurs et les adaptateurs Bus (HBA)
- *"Security Management to Fabric"* – Domaine entre les applications de gestion et les commutateurs.
- *"Switch to Switch"* – Domaine entre les commutateurs interconnectés

Que le choix se porte vers un produit de sécurité SAN autonome ou que vous choisissiez de bâtir votre propre solution basée sur les standards, la sécurisation du stockage réseau demeure complexe et l'apanage d'experts en architecture et sécurité. Seule la maîtrise de la sécurité et du SAN permettent la mise en place, la maintenance et le contrôle de réseaux de stockage fiables et sécurisés.