Chapitre 3
La sécurité dans l'entreprise - Les systèmes

1. Objectifs

Dans une entreprise, le plus important en termes de sécurité informatique consiste à protéger le système d'information et de le prémunir des risques potentiels. Cela signifie de mettre en œuvre un processus de gestion de sécurité pour tous les environnements logiciels (systèmes d'exploitation, applications...) et matériels (serveurs, infrastructure réseau...) présents dans l'entreprise et de pouvoir bénéficier des dernières améliorations en matière de sécurité.

2. La disponibilité des données et des systèmes

2.1 Concepts et principes

L'un des principes de sécurité qui doit être appliqué comporte la mise en place des environnements techniques et organisationnels de façon à garantir :

– la disponibilité des données, des applications et des services ;

– la tolérance aux pannes ;

– la prévention des incidents graves.

La finalité en relation avec ces bases consiste à définir et à implémenter principalement une protection sur plusieurs niveaux en considérant la disponibilité :

– des données (SAN, RAID, sauvegarde...) ;
– des systèmes (clusters, virtualisation...) ;
– des applications ;
– de l'infrastructure (énergie électrique, réseaux de communication).

2.2 La disponibilité des données

Différentes technologies sont utilisées pour assurer que celles-ci sont accessibles de façon permanente et sécurisées pour les applications utilisées par l'entreprise. Les solutions existantes sont présentées ci-dessous.

2.2.1 La technologie RAID (Redundant Array of Inexpensive Disks)

Elle est constituée d'un ensemble de disques durs indépendants qui permet de réaliser une unité de stockage. Selon le type de technique (à partir de RAID-1), l'unité ainsi créée possède une grande tolérance de panne avec un risque minimal de perte de données. La répartition des informations sur plusieurs unités permet donc d'augmenter la tolérance aux pannes, la sécurité et leur disponibilité.

Les disques assemblés en unité de stockage peuvent être utilisés de différentes façons, appelées niveaux RAID. Les formes les plus courantes sont listées ci-dessous :

– **Niveau 0** ou striping ou agrégat de bandes.
– **Niveau 1** ou mirroring (disques disposés en miroir), shadowing.
– **Niveau 3** ou grappes de disques identiques, une unité de stockage est réservée à la gestion de la parité.
– **Niveau 4** : type amélioré du niveau 3 avec une gestion synchrone des unités de disques.
– **Niveau 5** : agrégat de bandes avec parité alternée (parité répartie sur tous les disques).

– **Niveau 6** : extension du niveau 5, utilisation d'une double parité répartie sur tous les disques.
– **Niveau 10** : assemblage de **niveau 0** et de **niveau 1**.

Actuellement, les plus utilisés sont les formes RAID-1, RAID-5, RAID-10.

Il existe des combinaisons de type RAID matériels et logiciels.

Le RAID logiciel

Cette technologie, basée sur le système d'exploitation, permet d'utiliser tous les types de disques équipant les serveurs sous différentes plateformes (Windows, Linux, Unix) pour créer des structures redondantes économiques et faciles à implémenter. Dans certains cas, l'assemblage sous cette forme logicielle est plus performant que le type matériel décrit ci-dessous. Plusieurs combinaisons de cette structure sont réalisables.

Tous les systèmes d'exploitation les plus courants de Windows à Unix, en passant par Linux permettent la création d'éléments de stockage sous forme de volumes RAID.

Le RAID matériel (via un module SCSI)

Dans ce cas, le principe d'agrégation est basé sur le matériel, en général une carte SCSI disposée dans le serveur. Le système est indépendant du serveur hôte et ne rend visible à celui-ci qu'une seule unité de disque par assemblage. Sa fonctionnalité est gérée entièrement par le module dédié pour l'écriture et la lecture, de même que pour la gestion des erreurs.

Ce dispositif se configure sur les serveurs comportant les unités de disques durs, une carte d'interface est prévue à cet usage. Il existe alors des outils de configuration pour les regrouper selon l'architecture RAID désirée.

Il est alors possible de paramétrer un assemblage de RAID de niveau 1 pour y installer le système d'exploitation. Les fichiers seront disponibles physiquement simultanément sur les deux disques durs de la configuration.

En cas de défaut de l'un d'eux, le serveur pourra alors continuer à fonctionner normalement car au moins un des deux est présent.

Toutefois, il est important de prévoir un outil de supervision qui va détecter que l'une des deux unités est défectueuse, informer l'administrateur du système pour qu'il prévoie une intervention au niveau du matériel. En l'absence de cette alarme indiquant le défaut, le système peut s'arrêter complètement de fonctionner de façon inopinée si le second disque dur devient à son tour hors d'usage.

Remarque

Il est requis d'effectuer la supervision des évènements (gestion des erreurs et des alertes) survenant sur les disques faisant partie d'un miroir (RAID-1 pour Windows), principalement s'il s'agit des supports sur lesquels est installé le système d'exploitation.

En effet, l'un des deux peut avoir une défectuosité et ne plus être utilisable, sans que l'accès au système d'exploitation ou aux applications ne soit affecté. Le défaut existe mais il n'est pas visible. Quand un incident arrivera sur le deuxième disque du miroir (RAID-1), l'accès sera interrompu et le système s'arrêtera ou bien les données en cours de traitement ne seront plus accessibles. Ce qui amènera à l'arrêt brutal du système ou de l'application.

2.2.2 Le réseau de stockage SAN (Storage Area Network)

Ce concept permet le stockage des informations et leurs échanges entre plusieurs serveurs et périphériques, d'assurer une meilleure disponibilité d'accès aux données et de garantir la tolérance aux pannes. Ces données n'ont pas besoin d'être transférées par le réseau local d'entreprise (LAN) pour être accessibles par l'intermédiaire de plusieurs machines.

Une telle architecture se compose de serveurs, de périphériques de sauvegarde, d'éléments de stockage, de baies de disques, tous reliés par une connexion réseau rapide (généralement Fibre Channel). Son déploiement facilite la mise en place d'une stratégie complète de stockage au sein d'une entreprise.

Elle permet l'interconnectivité de l'ensemble des ressources : les périphériques peuvent alors être partagés entre plusieurs systèmes client, le trafic de données ainsi que la disponibilité des périphériques sont améliorés.

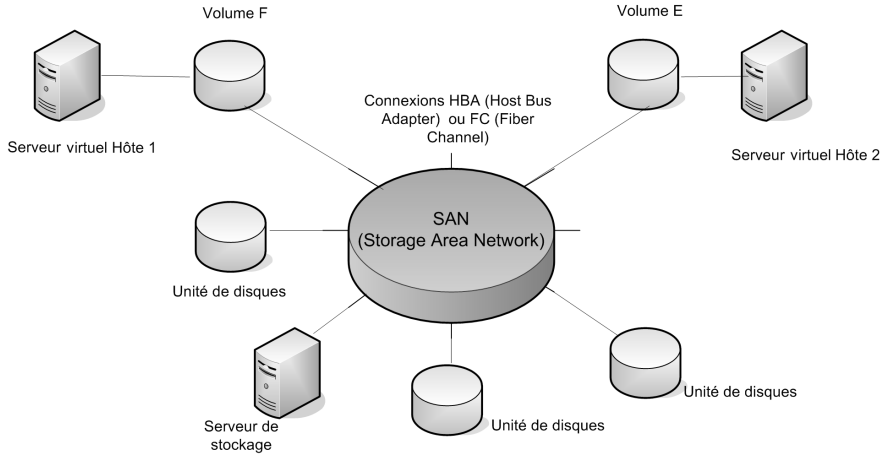
Le partage de l'espace disque s'effectue entre les différentes plateformes qui y sont connectées, il simplifie l'administration (création et gestion de zones de stockage) et rationalise les opérations de sauvegarde.

Cette unité est reliée à un réseau dédié au stockage. La technologie est basée, le plus souvent, sur le standard Fibre Channel (1 à 128 Gbits/s). Elle permet l'interconnexion entre des serveurs et des baies de stockage.

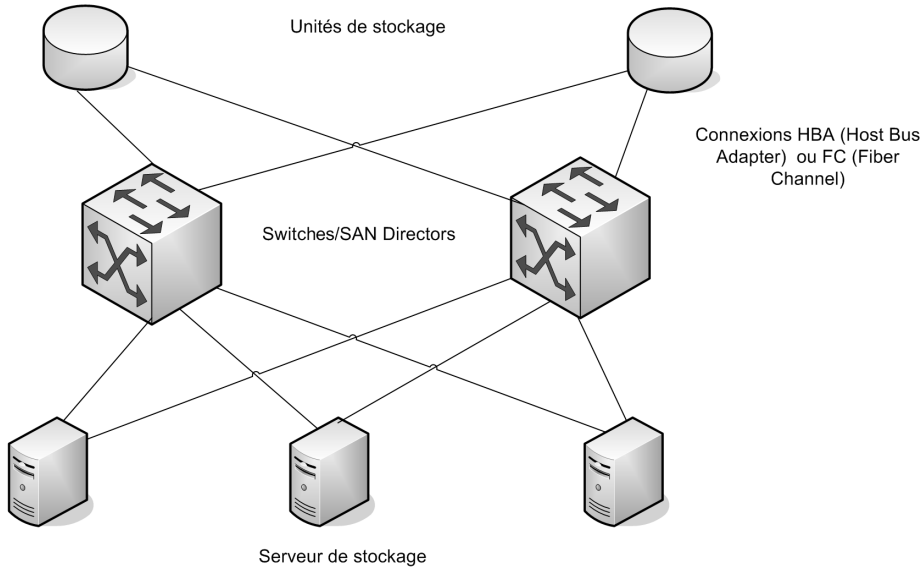
Dans un réseau de type SAN, il est possible de connecter de nouveaux serveurs ou d'ajouter de nouvelles capacités de stockage sans perturber les autres systèmes ni interrompre l'accès aux données.

Dans le cadre d'une telle architecture, il existe trois topologies possibles :

– Point à Point : permettant de relier deux éléments avec un débit à partir de 1 Gbits/s ce qui correspond à une bande passante effective de 100 Mo/s et une distance pouvant aller jusqu'à 10 km.
– FCAL : *Fibre Channel Arbitrated Loop* (arbitrage de boucles). Les informations transitent d'une manière séquentielle. Toutefois, la déconnexion d'un élément en fonctionnement n'est pas supportée.
– Switché : le mode Fabric est une configuration comportant un ou plusieurs switches Fibre Channel interconnectés. Cette topologie est la plus performante.



Configuration classique d'un réseau SAN



Exemple de configuration d'une architecture de type Fabric

Les connexions associées au SAN

Ces liaisons **point à point** ou **FCAL** sont réalisables sur de longues distances selon deux modes :

– Lien optique Fibre Channel reliés par deux switches.
– Lien IP jusqu'à plusieurs milliers de kilomètres, utilisable principalement en l'absence d'infrastructure de fibre optique.

En effet, le lien optique utilise les technologies FCoE (*Fibre Channel over Ethernet*) et iSCSI (*SCSI over IP*), ce qui autorise les communications à l'aide d'un réseau IP standard via Fibre Channel Tunneling. Ce type de lien permet d'atteindre des limites de distance jusqu'à 10 km quand des fibres optiques sont utilisées.

Les constructeurs et éditeurs de logiciels s'appuyant sur la technologie SAN proposent des outils adaptés pour chaque configuration. Ceux-ci permettent de définir un environnement de sécurité sous la forme de :

– Zoning : c'est une méthode d'organisation des périphériques connectés en Fibre Channel en groupes logiques à partir de la configuration physique. Elle permet la limitation et le contrôle du trafic entre l'adaptateur FC (*Fibre Channel*) installé sur le serveur (host) et l'unité de stockage attachée. Le zoning peut être de type matériel ou logiciel, implémenté pour compartimenter des ensembles ou structures de données, ce qui permet d'assurer leur intégrité.
– LUN (*Logical Unit Number*) : c'est une entité logique qui convertit un espace brut d'espace disque en unité de stockage logique que le système d'exploitation peut accéder et utiliser.

Le SAN et l'aspect sécurité d'accès aux données

Une amélioration est alors réalisable par la méthode du masquage de LUN (LUN masking). Cette solution permet de limiter le nombre de connexions sur une LUN et de pouvoir mieux les contrôler. Cette configuration fournit un environnement sécuritaire important surtout dans le cas de multiples connexions réseau.

Le réseau SAN possède une sécurité renforcée par rapport à un réseau LAN, dans lequel les données sont susceptibles d'être captées ou altérées. En effet, il existe peu de possibilités d'intrusion (le SAN étant séparé du réseau LAN), mais à partir du moment où un accès a été réalisé, le risque est accru (toutes les données peuvent être copiées ou détruites). De plus, tout dysfonctionnement du SAN provoque des interruptions dans les applications (forte sensibilité au niveau des SGBD).

Bonnes pratiques de mise en place d'un SAN : les questions à se poser

De par son concept, le SAN permet une meilleure disponibilité des données, ce qui implique quand même de prendre quelques précautions dans la réalisation de l'architecture. Il est donc nécessaire de considérer, en amont, les points suivants :

- Si le SAN est utilisé dans le cadre d'une virtualisation d'application, il est important de se poser quelques questions simples : quelles applications vont être exécutées sous un environnement de machines virtuelles et combien y en a-t-il par serveur connectées au SAN ?
- Dans le cadre d'une sauvegarde et de la tolérance aux pannes du matériel :
  - Y a-t-il une sauvegarde centralisée ?
  - Quel est l'impact des applications critiques sur la sauvegarde ?
  - Une solution, dans le cas d'un sinistre, basée sur une infrastructure Metro Fibre Channel ou FCIP (*Fibre Channel over IP*) est-elle prévue ?

Règles de base de sécurité à prévoir au niveau du SAN

Il est recommandé de le protéger physiquement :

- Changer les mots de passe définis par défaut par le constructeur/éditeur.
- Créer un réseau séparé pour l'administration (sur les serveurs concernés).
- Bien configurer le zoning.
- Inhiber les ports non utilisés des switches du réseau SAN.
- Bien documenter et sauvegarder sa configuration.
- Repérer et documenter toutes les connexions entre les différents composants.
- Mettre en place une supervision et la possibilité d'alertes.