Sécurité et Réseaux de Stockage

François Riche
Consultant Indépendant
lundi 20 mars 2006
OSSIR/ReSIST

Présentation des aspects sécurité du SAN

Qu'est-ce que le SAN ?
Composantes SAN proches de la sécurité
Sécurité SAN, état de l'art à ce jour
Sécurité SAN, les fabricants :
Brocade, Cisco, McData

Introduction au Réseau SAN

SAN en quelques mots :
définitions, vocabulaire,
protocoles, adressage

SAN en quelques mots

- SAN: réseau pour le stockage
- réseau reliant :
  - serveur
  - baie de stockage
  - robotique de sauvegarde
- double liaison optique point à point
- liaison série, synchronisation par le flot
- maillé par des commutateurs électroniques
- assemblage automatique de commutateurs

SAN en quelques mots (suite)

- protocole « Fiber Channel »
- pour le transport de données en mode bloc
- protocoles SCSI, ESCON, (IP)
- train de trames de 2KB maximum
- assure la non perte de trame
- assure l'arrivée des trames dans l'ordre
- latence faible de la µs à la ms
- réseau sous-utilisé mais disponible

Protocole FC du SAN

- découpage en trame des bloc d'IO
- structure : session, séquence, trame
- adressage des composants SAN
- règles d'assemblage et de reconstruction automatique de la fabric
- routage des trames FC dans la fabric
- serveur de noms distribué

Commutateur SAN

- machine avec des ports FC
  - port banalisé : U, FL, G, F, E..
  - port(s) IP, port(s) série, prise(s) électrique(s)
- chaque port FC reçoit un SFP
  - SFP convertisseur optique/électronique
  - SERDES convertit le flot de bits en trames FC
- ASIC route les trames entre ports
  - table de routage, zoning hardware
- UC héberge l'OS et le fabric OS (microcode)
  - fabric OS permet la gestion du SAN
    - administration commutateur et fabric
    - gestion automatique de la fabric

Vocabulaire du SAN

- switch, dénomination physique d'un commutateur
- domaine, dénomination logique d'un commutateur
  - switch divisé en plusieurs domaines par VSAN
- directeur, gros switch >100 ports + qualités de tolérance aux pannes
- ISL, liaison entre deux domaines
- fabric, assemblage automatique de domaines par lien ISL

Vocabulaire du SAN (suite)

- WWN, équivalent de la MAC adresse
- HBA, Host Bus Adapter
  - matériel périphérique de connection
  - n'assure pas de ré-émission
- zone, ensemble de périphériques SAN autorisés à communiquer ensemble
- RSCN, alerte émise par un élément
  - switch, broadcast à toute la fabric
  - HBA, multicast aux éléments de la zone

Adressage dans le SAN

- adresse composite domaine + port (24 bits)
- par identificateur de domaine dans la fabric (8 bits) (239 domaines max)
- par identificateur de port dans chaque domaine (8 bits) (256 ports max)
- voire par identificateur de port d'une boucle FC-AL (7 bits) (126 ports max)

WWN : World Wide Name

- équivalent de la MAC adresse
- définition IEEE sur 128 bits
- numéro(s) réservé(s) par fabricant
- ne devrait pas être modifiable/masquable
- serveur de noms distribué associant un WWN à un domaine/port
- pilote HBA utilise WWN (Solaris, Windows) ou domaine/port (AIX, HP/UX, mainframe)

Protocoles du SAN

- SCSI
  - FC évolution sur fibre optique du SCSI
  - jeu de commande SCSI inchangé
- FICON
  - FICON évolution sur FC de l'ESCON
  - jeu de commande ESCON inchangé
- IP
  - encapsulation IP dans FC
  - peu ou pas utilisé, supporté par [BCM]

Fabricants/Fournisseurs

- fabricants de commutateurs
  - Brocade, CISCO (gros commutateur), McData, Qlogic (petit commutateur)
- fabricants de HBA
  - Emulex, Qlogic
- fournisseurs : commutateurs, HBA
  - tous: Bull, Dell, EMC, Hitachi, HP, IBM, NetApp, STK, SUN
  - revendeurs : leurs partenaires

Autres éléments du SAN

Important pour l'aspect sécurité :

zoning, administration, longue distance (FC et IP), VSAN et routage

Zoning

- ensemble de périphériques SAN
- aucune notion de routage incluse
  - pas de possibilité de forcer un chemin
- les zones peuvent se recouvrir
- ajout/retrait/modification de zones par nouvelle configuration
- nouvelle configuration non-disruptive pour éléments autorisés à se voir avant et après
- une zone contient les RSCN de ces éléments

Implémentation interne zoning

- ≠ technologies de commutation
  - cut-through [BM]
  - store-and-forward [C]
- zoning, rejet de la trame
  - egress port pour cut-through
  - ingress port pour store-and-forward

Administration du SAN

- se fait en outband (inband possible)
  - par un réseau IP
    - voire liaison série pour maintenance
  - excepté pour les mainframes, en inband
- plusieurs possibilités IP
  - en mode commande avec telnet
  - en mode graphique avec un butineur
  - en mode RPC (API) pour frameworks type ECC/Tivoli/OpenView/…

Administration du SAN (suite)

- administration de chaque switch
  - possède ses mots de passe
  - possède ses paramètres
  - possède ses audits et ses alertes
- administration de la fabric
  - de chaque switch
    - configuration du zoning
    - modification du serveur de noms

Administration SAN (suite et fin)

- configuration de l'audit
  - positionnement d'alertes
    - surveillance du matériel
    - sécurité classique
    - surveillance des erreurs (lien, élément)
    - surveillance des débits
- externalisation des audits
  - par snmp (V1, V2, V3) [BCM]
  - par syslog [BCM]

Longue distance lien optique FC

- 2 commutateurs reliés par une liaison optique FC longue distance
  - utilisation de fibre monomode
- de 1km à max 100km, fibre noire
  - utilisation de SFP Long Wave Length
- de 10km à 1000 de km avec des opérateurs Telco (fibre optique)
  - utilisation de techniques DWDM/CWDM

Longue distance lien IP

- entre 0 et plusieurs milliers de km, utilisée
  - en l'absence d'infrastructure fibre optique
  - ou pour réduire le coûts
- encapsulation IP : 2 solutions
  - protocoles FCIP et iFCP
  - jumbo frame à cause de MTU IP à 1500 max
- gère la non-perte de trame et l'ordre d'arrivée de trames
- engendre de la latence de 20µs à 50µs si compression; à multiplier par 2
- crypto externe Neoscale, Decru : 2x 100µs

FCPI et iFCP

- FCPI
  - liaison point à point
  - simule un lien ISL, même fabric
  - encapsulation IP de trame FC
- iFCP
  - liaison multipoint
  - routage IP de trame FC
  - commutateurs dans fabrics différentes
  - routage FC : modification de trame FC

Virtual SAN

- très comparable au VLAN
  - dans l'implémentation CISCO
  - domaine d'administration pour Brocade
  - Zone Flexpar pour McData
- compartiment étanche comparé au zoning
  - pas de recouvrement
- pas de déplacement d'un périphérique SAN entre « VSAN » sans rompre la liaison

Routage entre fabrics

- 3 fabricants, 3 solutions
  - FC routeur de Brocade
  - Inter VSAN Routing de CISCO
  - iFCP de McData
- évolution de l'adressage plat
- administration du routage
  - par administrateurs SAN interconnectés
  - par administrateur fonction routage FC
  - par administrateur fonction routage IP

Framework d'administration

- malgré frameworks des fournisseurs, chaque fabricant a développé le sien
- application externe hebergée en dehors du SAN
  - Brocade Fabric Manager
  - CISCO Fabric Manager
  - McData EFCM
  - hebergée sur un serveur externe
  - paramètres fabric conservés hors fabric

Ne pas confondre SAN et ?

- NAS
  - transport mode fichier
  - protocole au-dessus de IP : NFS, CIFS
- iSCSI
  - transport en mode bloc
  - protocole SCSI au-dessus de IP
  - utilise la notion d'IQN, sorte de WWN
  - pour intégration du monde Windows et Linux à utiliser les ressources du SAN

Acronymes

- SFP Small Form-factor Pluggable
- ASIC Application Specific Integrated Circuit
- SERDES SERializer DESerializer
- SCSI Small Computer System Interface
- HBA Host Bus Adapter
- ISL Inter Switch Link
- RSCN Register State Change Notification
- LUN Logical Unit Number
- RBAC Role Based Access Control
- SSH Secure Shell
- SSL Secure Socket Layer
- RADIUS Remote Authentication Dial In User Service
- TACACS Terminal Access Controller Access Control System
- SNIA Storage Networking Industry Association
- FC-SP Fiber Channel Security Protocol
- CHAP Challenge Handshake Authentication Protocol
- NAS Network Architecture Storage

Sécurité élémentaire du SAN

SAN très peu popularisé

SAN en milieu physiquement protégé

SAN très robuste (réduit l'expérience donc la connaissance)

Faible chance mais grand risque

- il y a peu de chances d'intrusion
  - peu ou pas de cas connu
- si intrusion, tout peut être copié
  - copie, peut-être invisible
  - destruction, visible rapidement
  - modification, plus difficile
- protection aux erreurs humaines
  - premier motif pour la sécurité du SAN
- SAN s'échappe du stockage

Sécurité réseau/sécurité SAN

- peu d'initiés; si initié, faible expérience
- faible connectivité <100 ports
- dysfonctionnement du SAN fait planter les applications (SGBD très sensible)
- gestion SAN comparable au mainframe
  - maintenance programmée
  - si ça marche, ça marche. On ne joue pas
- standard SNIA T11 FC-SP draft

Sécurité SAN et IP

- IP sur FC n'est quasiment pas utilisé
  - faible chance de ponter IP avec du SAN
- FC sur IP
  - utiliser l'armement sécurité IP
  - utiliser le chiffrement IP externe
- iSCSI
  - risques potentiels à l'intérieur de la zone des éléments iSCSI (usurpation d'IQN)
  - sujet à développer

Règles de base sécurité SAN

- protéger physiquement le SAN
- changer les mots de passe fabricant
- créer un réseau séparé IP d'admin du SAN
- configurer le zoning
  - tendance aux petits commutateurs pré-zonés
- ports non utilisés : inhiber ou ISL interdit
- documenter le SAN
- labelliser les connections
- mettre en place des alertes

Gestion des comptes admin

- risque
  - compte(s) standard
  - mot de passe usine
- solutions
  - changer les mots de passe usine (qualité)
  - comptes admin avec rôles, RBAC [BCM]
  - unifier, centraliser, déporter la gestion
    - interne [B], Radius [BCM], TACACS [C]
  - auditer toutes les actions

Télémaintenance

- risque
  - modification zoning par télémainteneur
  - pas possible d'accéder aux données
  - collusion avec utilisateur interne
- solutions
  - limitation à la téléalerte
  - télémaintenance contrôlée
    - ouverture liaison par client, double écran, audit, limitation des rôles d'admin (RBAC)

Espionnage IP des comptes

- risque
  - lecture les sessions admin des liaisons IP
    - vol des comptes/mots de passe
    - vol des paramétrages de configuration
- solutions
  - séparer réseau IP d'administration SAN
  - utilisation de telnet sécurisé (SSH)
  - utilisation de copie sécurisée (SCP/SSH)
  - utilisation de WEB sécurisé (SSL)

Zoning

- zoning par port ou par WWN
- zoning dit harware enforced [BCM]
- zoning par port
  - connecter un nouvel élément à la place
  - facile si une HBA tombe en panne
- zoning par WWN
  - utiliser les alias pour panne de HBA
  - se protéger contre usurpation de WWN

Zoning par WWN et usurpation

- risque
  - beaucoup de discussions
  - peu d'expérience, pas de cas connu
- solutions
  - inhiber les ports inutilisés
  - association WWN<->port [BCM]
  - CHAP entre commutateurs et HBA [QE]
    - très bientôt

LUN Masking

- disques durs d'une baie recomposés en unités logiques appelées LUN
- LUN masking : masque des LUN
- au niveau du serveur
  - très déconseillé
- au niveau du SAN
  - peu utilisé [C]
- au niveau des baies
  - administration stockage des accès aux données
  - très conseillé

Switch pirate

- risque
  - introduire commutateur pirate dans une fabric
  - facile à réaliser
- solutions
  - ports inutilisés : inhiber ou ISL interdit
  - définir les commutateurs d'administration
  - utiliser fabric binding [BCM]
    - CHAP entre commutateurs
    - liste des commutateurs de la fabric

SAN et Deni de Services

- risque
  - saturer un accès disque
  - lien saturé par un seul serveur, difficile
  - serveur non-autorisé sur port disque, difficile
- solutions
  - audit détection dépassement seuil bande passante : 50% conseillé
  - store-and-forward bloque trafic ingress
  - blocage sur abus : port fencing [M]

Fabricants de Commutateurs SAN

Brocade
CISCO
McData

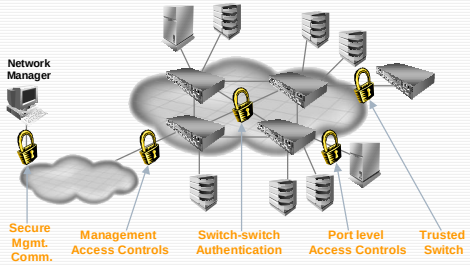
Sécurité Brocade

- Secure Fabric OS
  - offre sécurité ancienne 5 ans
  - généralisée et relancée pour FICON 3 ans
- option payante, évolution en cours
  - centralise la BD des comptes et des règles
  - un serveur d'administration + serveur(s) secours
  - CHAP entre commutateurs + domain binding
  - contrôle d'accès IP et physique aux commutateurs
  - audit et alertes très développés
- plus d'éléments SFOS intégrés dans FOS
  - multiple comptes + RBAC
  - Radius

Secure Fabric OS Benefits

- Secure the SAN infrastructure from unauthorized management and device level access
- Share resources within the same fabric by tightly controlling where devices (servers/hosts) can attach
- Provide a secure means for distributing fabric wide security and zoning information (trusted switch)
- Create a 'trusted SAN infrastructure'

Secure Fabric OS Components



Sécurité McData

- SANtegrity
  - offre sécurité ancienne avec SANtegrity binding
- option payante, évolution en cours
  - SANtegrity intègre maintenant
    - RBAC
    - CHAP
    - Zone Flexpar
    - Crypto (à venir)

McDATA Security Solutions

- Reduce Accidental Connections :
  - Device Authorization (Hardware enforced zoning, SANtegrity Binding)
  - User Authorization – Role Based Access Control
  - Centralized management (EFCM / Security Center)
- Protect Management Interfaces
  - Lock down the IP management interfaces (SSH, SSL, IP ACL)
  - Isolate Management Zone from Corporate Network (Architecture)
  - Protect / Manage usernames and passwords (Radius, encryption)

McDATA Security Solutions

- Reduce the risk of Denial of Service attacks
  - High Availability (Unit Design)
  - ISL Port Fencing – block a port based on threshold violation
- Protect the network from malicious WWN Spoofing
  - SANtegrity Binding
  - SANtegrity CHAP Authentication
- Communication Protection
  - Physical Security or Privacy
  - IP Encryption? FC Encryption

Sécurité CISCO

- translation de l'expérience IP
  - VLAN/VSAN, serveur d'authentification…
- offre sécurité developpée
  - notamment à tous protocoles proches d'IP comme par exemple iSCSI

Vision Cisco pour la Sécurité

Considérations de base

- La politique de sécurité pour le Réseau de Stockage doit s'intégrer dans la politique de sécurité globale de l'Entreprise
- La sécurité doit être centralisée pour garantir un contrôle et une efficacité accrue et autoriser une mise en œuvre de bout en bout – RADIUS et TACACS+
- Ne pas réinventer la roue à Utiliser des mécanismes de partitionnement et sécurité ayant fait leurs preuves dans les autres types de réseau. Ex.: VSAN/VLAN – ACL/Zoning – IPSec/FC-SP…
- Dimensionner le plan de contrôle (Control plane) des équipements en conséquence. Ex.: le chiffrement des flux d'administration ne doit pas pénaliser le traitement des events pur FC, aussi bien provoqué (zoning change) ou imprévu (RSCN processing, etc.)
- Filtrage de trame et imposition de label (Virtual fabric) traités en hardware sans impact sur les perfs. Commutation et Routage intégrés à filtrage unique

Vision Cisco pour la Sécurité

- Les principaux domaines traités
  - Administration : authentification et chiffrement, SSHv2, SFTP, SCP, SSL pour SMI-S, SNMPv3
  - Authentification de tout nouvel entrant pour accéder aux ressources du Réseau de Stockage
  - Protocole de communication sécurisé entre nœuds réseau
  - Filtrage par ACL en entrée du Réseau – protection contre les attaques de type DoS. LUN Zoning contre les DoS attacks vers les baies. Utilisation de Ternary CAM – 20K entrées par ACL
  - Authentification des ressources iSCSI et peers FCIP et chiffrement des flux
  - Support d'IPv6 pour l'administration, iSCSI et FCIP

Conclusion

- offres fabricant satisfaisantes
  - pour assurer un bon niveau de sécurité
  - quelque soit le fabricant [BCM]
- mise en pratique sécurité insuffisante
  - de la part des clients
  - de la part des fournisseurs
  - problème de formation
- voire offres fabricant très en avance sur la demande client

Merci de votre attention

François Riche
riche@orange.fr
+33 681 629 641