WebSphere. software

Guide MQ du 21/03/2003

Sécurité WebSphere MQ V 5.3

Luc-Michel Demey

Demey Consulting

lmd@demey-consulting.fr

Plan

- Les besoins
- Les technologies
- Apports de la version 5.3
- Mise en œuvre
- Cas pratiques
- Intérêt et limites

WebSphere. software

WebSphere MQ et la sécurité

Les Besoins

Sécurité MQ : Les besoins (1)

- Contrôle des droits d'accès aux objets MQ
  - Queues
    - droits d'utilisation (put, get, …)
    - droits d'administration (alter, clear, …)
  - Channels
    - Droits d'administration (start/stop, alter, …)
      - Exits de channel (record / chg du flux)

Gestion de ces droits par l'OS (+MQ)

Sécurité MQ : Les besoins (2)

- Droits d'administration
  - Administration locale
    - Gestion par les droits OS + MQ
  - Administration distante
    - Ouverture du Command Serveur : comment filtrer les accès ?
- Clients MQ
  - Identification ?
  - Client Java !

Sécurité MQ : Les besoins (3)

- Sécurité Niveau Transport (channels)
  - Entre clients et serveurs
  - Entre serveurs

  – Identification du partenaire
  – Intégrité des données
  – Confidentialité des données

Sécurité MQ : Synthèse des besoins

- Authentification
  - Niveau utilisateur (quel user ?)
  - Niveau QM (quel serveur ?)
  - Niveau client (quel poste / user ?)
- Intégrité
  - Niveau Queue (contenu)
  - Niveau Channel (ligne)
  - Niveau configuration (Alter ...)
- Confidentialité
  - Niveau Queue
  - Niveau Channel (ligne)
- Non-répudiation
  - Niveau message ***applicatif***

WebSphere. software

WebSphere MQ et la sécurité

Les Technologies

Les technologies

- Commandes MQ niveau OS : *setmqaut*
- Exit de sécurité niveau channel
- Scellement de messages
- Chiffrement de messages
- Certificats, PKI, SSL

Scellement

Principe : détecter toute altération d'un flux

- Calcul d'un hachage du flux (MD5, SHA, …)
- Ajout du hachage au flux en tant que *trailer*
- A l'arrivée, re-calcul du hachage :
  - MD5 = trailer : le flux est intact
  - MD5 # trailer : le flux a été altéré

Problème : et si le pirate recalcule le hachage ?

Chiffrement

- Clés secrètes
- Clés asymétriques (bi-clé)
- Certificats

Chiffrement – Clés secrètes

- Chiffrement symétrique
- La même clé est connue des deux correspondants (mot de passe)
- Cette clé sert à chiffrer et à déchiffrer un flux
  - Exemples : DES, IDEA, RC2, RC4, …

Problème : gestion & diffusion des clés

Chiffrement – Clés Asymétriques

- Pour un utilisateur, on a deux clés reliées par une relation mathématique
- Ce qui est chiffré par une clé peut être déchiffrée par l'autre (et vice-versa)
- Bi-clé :
  - clé publique (largement diffusée)
    +
  - clé privée (conservée par le propriétaire)

- Utilisation :
  - Chiffrement
  - Signature (authentification)

Clés Asymétriques : utilisation en chiffrement

Exemple :

- Bob veut envoyer une information confidentielle à Alice
- Bob chiffre son message avec la clé publique d'Alice
- Seule Alice pourra déchiffrer le message, grâce à sa clé privée

Clés Asymétriques : utilisation en signature

- Alice veut « signer » un message envoyé à Bob.
- Alice crée un hachage de son message, chiffre le résultat avec sa clé privée, et ajoute le résultat chiffré au message.
- Bob, à la réception du message :
  - recalcule le hachage à partir du message , et obtient S1
  - déchiffre, avec la clé publique d'Alice le hachage reçu dans le message, et obtient S2
- Si S1 = S2 :
  - C'est bien Alice qui a envoyé ce message
  - Et il n'a pas été altéré durant le transport
- Si S1 # S2 : Expéditeur incorrect ou message altéré !

Synthèse clés asymétriques

- La combinaison *chiffrement* + *signature* permet :
  - la confidentialité des échanges
  - L'authentification des correspondants

mais ...

- Le chiffrement asymétrique est très lourd en calcul
  - Chiffrement via clé symétrique générée à la volée, envoyée au partenaire chiffrée en asymétrique
- On authentifie la clé, pas son propriétaire !
  - Mise en place des certificats

Les certificats

Besoin : identifier l'utilisateur d'une clé

- Certificat :
  - Carte d'identité électronique
  - Contient la clé publique du propriétaire
  - Contient des informations sur le propriétaire

    (nom, département, société, adresse, mail, …)
  - Contenu certifié (« scellé ») par une autorité de certification (CA), publique ou privée
- Norme X509
- Délivrés par une CA commerciale ou interne

Public Key Infrastructure

- Infrastructure pour :
  - Générer les clés
  - Certifier les clés publiques (certificats)
  - Distribuer et révoquer les certificats
- Logiciels du commerce
- Logiciels Open Source
  - Open SSL

SSL – Secure Socket Layer - V3

Permet l'échange sécurisé de données sur TCP/IP

- Utilise :
  - Le chiffrement par clé symétrique
  - Le chiffrement par clé asymétrique
  - Les certificats
- Apporte :
  - La confidentialité des échanges
  - L'intégrité des échanges
  - L'identification du partenaire
- Exemples :
  - SSH (« Telnet » sécurisé)
  - Certificats des serveurs Web
  - Tunnels IP entre routeurs, VPN, ..
  - Et bien sûr WebSphere MQ version 5.3

WebSphere. software

WebSphere MQ : Apports de la version 5.3

Apports de WebSphere 5.3

- Outil de manipulation des certificats
  - iKeyman / MQExplorer / amqmcert / DCM
- Chiffrement des échanges channels en SSL V3
  - Pour toutes les plates-formes 5.3 client et serveur
- Mots-clés niveau Queue Manager / Client
  - Association d'un keyring au QM /client
- Mots-clés niveau channel
  - SSLCIPH (RC4_MD_US, DES_SHA_EXPORT, …)
  - SSLPEER (…) (filtre par DN)
  - SSLAUTH (REQUIRED | OPTIONNAL)

WebSphere. software

WebSphere MQ 5.3 & SSL

Mise en œuvre

Mise en œuvre du SSL

Trois étapes :

- Certificats & Clés
- Magasin de clés
- Modifications WebSphere MQ

Certificats & Clés

- Certificat du CA (Certification Authority)
  - En format .CRT
- Certificat personnel
  - Pour chaque Queue Manager
  - Pour l'utilisateur (si client MQ)
  - En format PKCS12

Le FriendlyName du certificat personnel doit être :

- ✓ Si Unix ou AS/400 : ibmwebspheremq<nom_qm>
- ✓ Si client Unix : ibmwebspheremq<profil_utilisateur>
- ✓ Si z/OS : ibmwebsphereMQ<nom_du_qm>

Magasin de clés

Synonyme : Certificate Store, Keyring, key repository

- Unix : Création / Gestion par iKeyman
  (livré avec WebSphere MQ, WAS, IHS, Tivoli, …)
  Existe en mode commande ou en graphique X11
- Windows :
  - *amqmcert* (mode commande)
  - Via l'explorateur WebSphere MQ (si Queue Manager)
- AS/400 : DCM - Digital Certificate Manager
  - Via un navigateur web, sur les ports 2001 ou 2010
- z/OS : gestion par RACF

Modifications WebSphere MQ

- Affectation du keyring :
  - au Queue Manager : ALTER QMGR SSLKEYR( )
  - au client MQ : variable d'environnement MQSSLKEYR ou dans le MQCONNX
- Modification des channels :

  SENDER/RECEIVER ou SVRCONN/CLNTCONN :
  - Paramètres SSLCIPH(…) & SSLCAUT(REQUIRED)
- Affectation du certificat au client si MQ Client Win
  - Par numéro d'ordre dans le magasin de clé

Modifications WebSphere MQ

Paramètres optionnels

- Support du HW Crypto :
  ALTER QMGR SSLCRYPT
  Unités IBM 4758 et ICSF
  Hardware dédié sur HPUx, Solaris, Aix

- Support des listes de révocation
  - via LDAP

WebSphere. software

WebSphere MQ 5.3 & SSL

Cas Pratiques

Cas Pratique 1

- Secteur économique : distribution
- Contexte : échanges de bons de commande / livraison
- Systèmes : 2 x QM sur Win 2000 & Aix
- Objectif : confidentialité des flux
- Solution :
  - Passage en version 5.3
  - Génération de deux certificats autosignés (iKeyman)
  - Activation du SSL sur les channels

Cas pratique 2

- Secteur économique : Banque
- Contexte : Administration sécurisée de WebSphere MQ
- Systèmes : 6 Unix & 20 QM, postes WinNT
- Objectif : Limiter l'administration MQ aux seuls postes autorisés
- Solution :
  - Passage en version 5.3
  - Installation du client MQ & MO71 sur les postes WinNT
  - Génération d'un CA et de certificats personnels pour les utilisateurs NT et les QM (OpenSSL)
  - Activation du SSL sur un channel client dédié à l'adminsitration
  - Fermeture des autres channels SVRCONN
  - Certificats sur clé USB (en cours)

WebSphere. software

WebSphere MQ 5.3 & SSL

Intérêt et Limites

Intérêt du SSL sur WebSphere MQ 5.3

Le support du SSL :

- Apporte
  - Le chiffrement des liens (QM à QM / QM à client)
  - L'intégrité des données
  - L'authentification des partenaires
- Permet la sécurisation de l'administration distante
- Pour un coût très faible
  - Upgrade 5.3
  - Gestion des certificats
  - Ressources

Limites du SSL sur WebSphere MQ 5.3

- Attention aux performances si trafic élevé
  - Ségrégation du trafic par multi-channel
  - Unités de chiffrement hardware
  - Upgrade CPU
- Pas d'authentification de bout en bout
- Pas de protection des messages dans les queues (hors celle de l'OS et du *setmqaut*)
- Sécurisation des « *Certificate Store* »

Conclusion

- Fonctions attendues par le marché
- Relativement rapide à mettre en œuvre
  - Compétence WMQ + PKI nécessaire
- Offre un excellent niveau de protection
  - Pour les domaines considérés

Retrouvez cette présentation sur :

http://consulting.demey.org/

rubrique « Fiches Techniques »

Luc-Michel Demey
lmd@demey.org
+33 6 08 755 655