WebSphere MQ : Confidentialité des messages

Le besoin

Lorsque l'on échange des informations via WebSphere MQ, il est courant de vouloir protéger les messages contenant ces informations.

Par protection on entend ici :

- Confidentialité : éviter qu'une écoute du trafic ou une exploration du disque puisse révéler le contenu des messages
- Intégrité : s'assurer que les données en transit n'ont pas été, volontairement ou non, altérées ou modifiées
- Identification mutuelle du partenaire WebSphere MQ : s'assurer que le partenaire avec qui on ouvre un channel est bien celui qu'il prétend être.

Deux cas sont à considérer :

- Les messages en cours de transfert dans un channel (channel serveur à serveur, ou channel serveur à client)
- Les messages en attente de traitement dans les files d'attentes d'un Queue Manager (XmitQ au départ et queues locales à l'arrivée)

Protection des messages dans les channels

La version 5.3 de WMQ intègre la possibilité de chiffrement SSL pour l'échange sur les channels, entre deux QM ou entre un QM et un client MQ.

Ce mécanisme, basé sur une combinaison de chiffrement asymétrique (clé publique / clé privée) et de chiffrement symétrique (clé de session) permet d'assurer l'intégrité et la confidentialité des messages transmis, ainsi que l'authentification mutuelle des partenaires.

L'activation du SSL sur les channels entre deux Queue Managers, ou entre un Queue Manager et un client MQ, permet donc de satisfaire aux 3 besoins ci-dessus, à savoir Confidentialité, Intégrité, et Authentification.

Les contraintes sont les suivantes :

- Les systèmes source et cible des messages (de part et d'autre des channel SSL) doivent être en version MQ 5.3.
- Des certificats SSL doivent être générés pour chaque Queue Manager ou client MQ et installés dans ceux-ci.
- Le paramétrage des channels doit être modifié pour activer les fonctions SSL.

Contact : ftwmq2006@demey-consulting.fr - http://demey-consulting.fr

WebSphere MQ : Confidentialité des messages

Par contre aucun logiciel supplémentaire n'est nécessaire.

Pour autant, si les messages sont protégés par SSL durant leur passage dans les channels, cette protection n'existe pas avant (quand les messages sont en attente dans la XmitQ) et après (quand les messages sont arrivés dans la queue locale du système de destination).

Protection des messages dans les queues

Si l'on souhaite assurer la confidentialité et l'intégrité des messages en attente dans les queues, il y a deux grandes possibilités :

- Faire confiance à la sécurité d'accès du système d'exploitation et du Queue Manager local, en s'assurant qu'aucun profil (hormis « *mqm* » et « *root/administrateur* ») n'a la possibilité de lire ou d'écrire dans ces queues.

  C'est possible mais pas forcément évident à réaliser, cela suppose à la fois un contrôle étroit sur les comptes utilisateurs, et une mise en place fine des droits MQ via le *setmqaut*.

  Cette solution ne nécessite aucun logiciel complémentaire.

- Installer un produit spécifique permettant le chiffrement des messages dans les queues. Il y a encore quelques trimestres, plusieurs produits de ce type étaient disponibles. Le seul qui reste crédible aujourd'hui à mon avis est celui d'IBM, « Policy Director », et dont le nom actuel est TAM4BI (Tivoli Access Manager For Business Integration).

  Policy Director est un logiciel à installer au minimum sur la machine dont on veut protéger les queues, et éventuellement sur les autres systèmes source ou destinataires des messages.

  Le principe de fonctionnement est d'intercepter de manière transparente pour l'application les appels MQGet/MQPut, et de chiffrer/déchiffrer les messages à la volée. Le point fort et que ce logiciel ne nécessite aucune modification de l'application, contrairement à d'autres produits.

  Sa mise en place, sans être trop complexe, reste assez technique. Bien que ce logiciel puisse être utilisé à la place du chiffrement SSL pour protéger les messages durant le passage dans les channels (auquel cas il doit être présent sur les machines source et cible), il devrait être possible de limiter son utilisation à la protection des messages dans les queues, et se reposer sur SSL pour la protection des messages dans les channels.

Fin du document

Contact : ftwmq2006@demey-consulting.fr - http://demey-consulting.fr