Administration via l'Explorateur WebSphere MQ

Ce document présente l'utilisation de l'Explorateur WebSphere MQ, et en particulier sa capacité à administrer des Queue Manager distants. Il aborde également les problèmes de sécurité liés à l'administration distante.

Principe

La version Windows du logiciel IBM WebSphere MQ[1] est livrée avec un module d'administration, l'*Explorateur WebSphere MQ*. Sans avoir la puissance ni la portée d'outils d'administration du marché, cet explorateur permet, de manière graphique, de piloter des instances MQSeries (Queues Managers).

Le nom « *Explorateur WebSphere MQ* » est d'ailleurs totalement justifié, l'interface est très proche de l'explorateur Windows et totalement intuitive. Elle permet d'accéder, en quelques clics de souris, à la quasi-totalité des paramètres des objets MQSeries.

L'explorateur WebSphere MQ (*EWMQ* en abrégé) permet donc, pour autant que l'on utilise un id utilisateur ayant des droits suffisants, d'administrer le ou les Queues Managers d'un système Windows local.

Il peut aussi, et ceci est moins connu, administrer des Queues Managers distants, y compris s'ils sont situés sur des plates-formes non-Windows (OS/400, Unixes, …)

L'EWMQ est, à ce jour, livré avec le logiciel *IBM WebSphere MQ for Windows*, et n'est pas disponible séparément. Ceci signifie que pour disposer de l'EWMQ sur votre poste de travail, vous devez installer le produit au complet, et donc disposer de la licence correspondante. Pourtant, sur un plan technique, l'EWMQ utilise des fonctions de type « client MQ », en particulier pour administrer des Queues Managers distants.

Administration d'un Queue Manager local

La mise en place est extrêmement simple :

- Assurez-vous d'avoir ouvert une session sur votre poste Windows sous un profil appartenant soit au groupe des administrateurs, soit au groupe « mqm ».

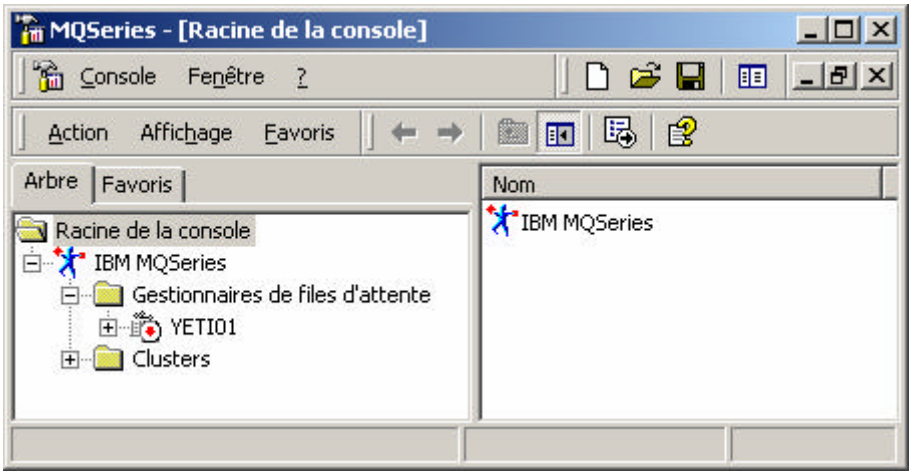
- Démarrer « Programmes / IBM WebSphere MQ / Explorateur WebSphere MQ »[2]. Vous obtenez une fenêtre comme ceci :

[1] Connu sous le nom « MQSeries » jusqu'en version 5.21

[2] « Programmes / IBM MQSeries / Explorateur MQSeries » jusqu'en version 5.21

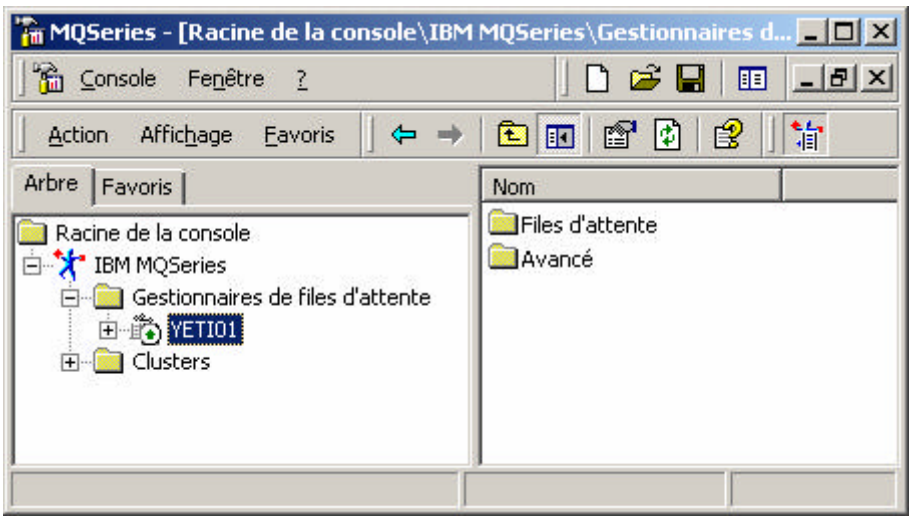
Contact : ftwmq2006@demey-consulting.fr - http://demey-consulting.fr

Administration via l'Explorateur WebSphere MQ



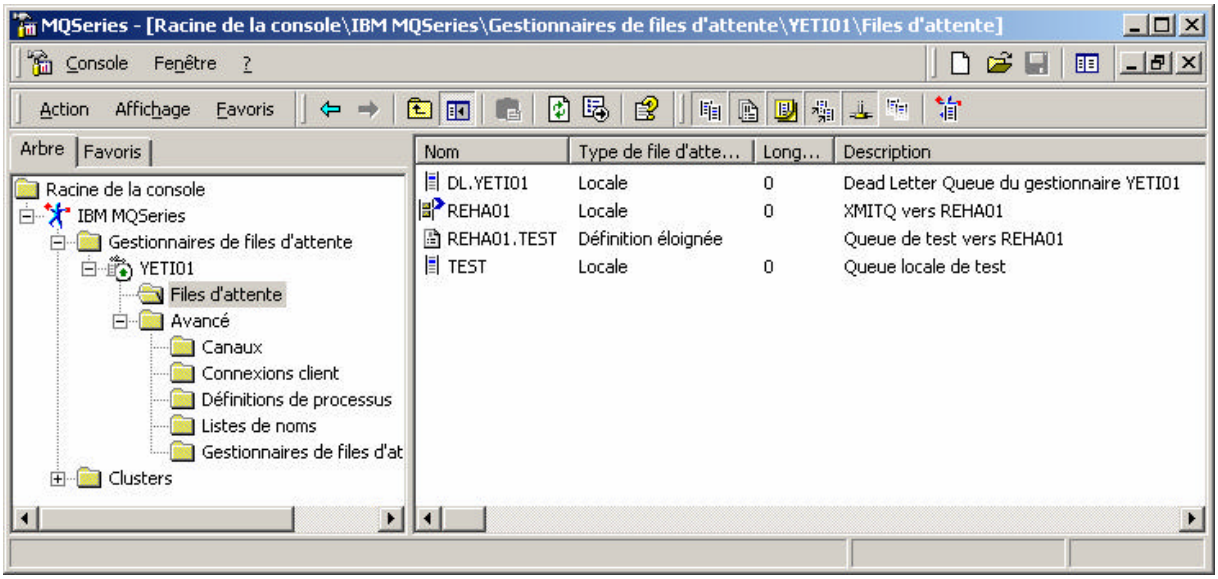
On voit ici qu'il existe un Queue Manager, nommé YETI01. La petite flèche devant le nom est rouge (pour ceux qui ont la couleur !) et tournée vers le bas, ce qui signifie que le Queue Manager est arrêté.

Un clic droit (Démarrage) permet d'obtenir le démarrage du Queue Manager :



Il est aussi possible de consulter la liste des queues ou le détail des paramètres :

Administration via l'Explorateur WebSphere MQ



A partir de ces écrans, vous pouvez créer, démarrer, arrêter, supprimer, visualiser le statut des différents Queues Managers résidant sur votre machine.

Vous pouvez également créer / modifier / afficher et même supprimer des queues, channels et process. Vous pouvez insérer ou lire des messages dans ces queues, démarrer et arrêter des channels, et connaître leur statut.

Conclusion

L'EWMQ est donc à la fois un outil très convivial et très puissant, qui permet à un non-spécialiste de configurer et de piloter complètement un ou plusieurs Queue Managers.

La création complète des objets d'un Queue Manager à travers l'EWMQ est très facile, mais dans ce cas on ne dispose d'aucune trace des opérations et surtout pas du fichier de commandes MQSC à rejouer pour recréer les objets si nécessaire.

Cette facilité même peut dans certains cas être considérée comme dangereuse. Il est en effet facile, d'un clic de souris, de supprimer ou de modifier les caractéristiques d'un objet MQ. Il peut donc être souhaitable de contrôler ou de limiter l'accès aux objets MQ via l'EWMQ, tout en conservant certaines fonctions pour leur convivialité.

Administration d'un Queue Manager distant

L'EWMQ ne permet pas seulement l'administration d'un Queue Manager local, il permet également celle de Queue Managers distants. Cela nécessite quelques opérations sur le système distant, puis sur le système Windows local.

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

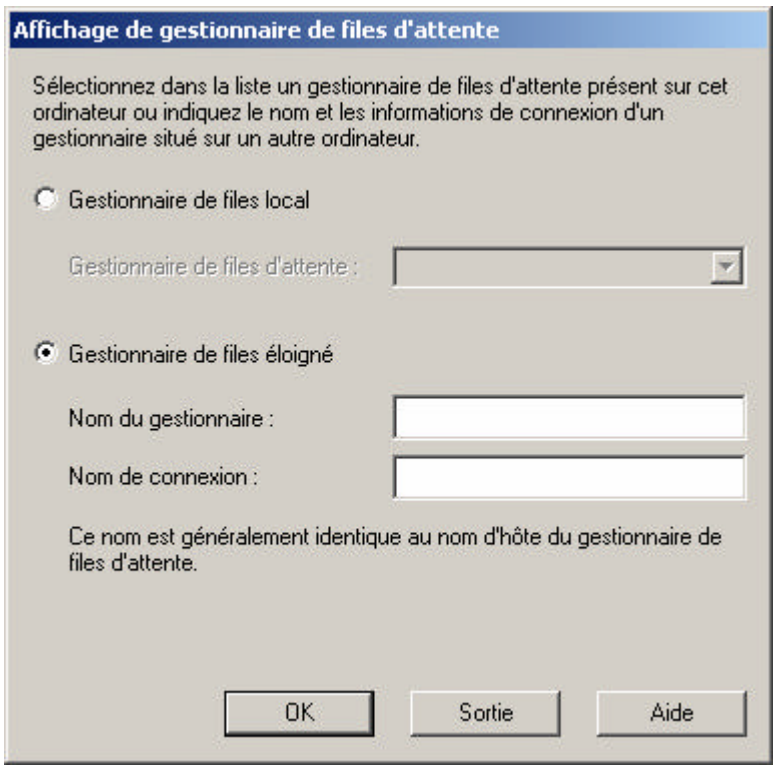
Administration via l'Explorateur WebSphere MQ

Opérations sur le système distant

- Vérifier la présence, et créer au besoin, le channel SYSTEM.ADMIN.SVRCONN, de type SVRCONN. Laisser les autres valeurs par défaut.
- Démarrer le serveur de commandes (*strmqcsv* si unix/NT)
- Vérifier que le listener IP est actif et noter le port d'écoute (1414 par défaut)

Opération sur le système local

- Ouvrez une session Windows avec un profil local appartenant aux groupes « mqm » ou « Administrateur ».
- A partir de la vue « Queue Manager » dans l'EWMQ, clic droit puis : « Affichage de gestionnaire de files d'attente » :



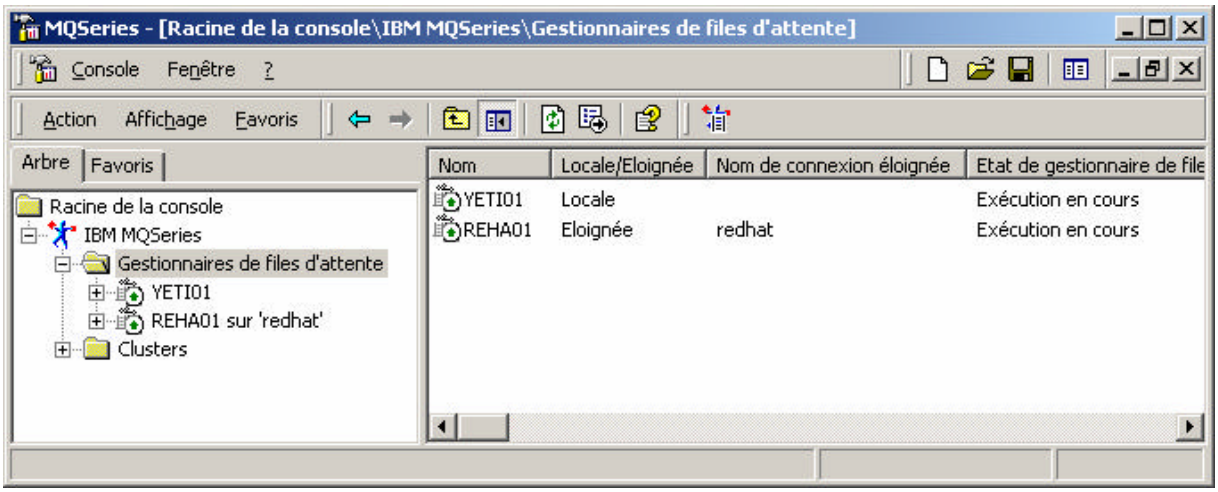
- Cochez la case « Gestionnaire de files éloigné », et dans la boite « Nom du gestionnaire », indiquez le nom du Queue Manager distant à afficher.
- Dans la boite « Nom de connexion », renseignez le nom IP (*hostname* ou adresse IP) du système sur lequel se trouve le Queue Manager. Si le port d'écoute du distant n'est pas la valeur par défaut 1414, il faut préciser le port d'écoute du *listener* entre parenthèses.

Administration via l'Explorateur WebSphere MQ

- Par exemple, pour administrer un Queue Manager nommé REHA01, sur le système « redhat », et dont le port d'écoute du listener est 1415, on rentre :

Nom du gestionnaire :	REHAT01
Nom de connexion :	redhat(1415)

Si, sur le système distant, il existe un profil ayant le même nom que votre profil local, et que ce profil distant appartient également au groupe « mqm » ou « Administrateur », c'est terminé et on obtient un écran comme celui-ci :



Si par contre votre profil local n'est pas connu sur le système distant ou n'a pas les droits MQ suffisants, une étape de configuration supplémentaire est nécessaire (cf. chapitre suivant).

Il devient possible d'administrer, à travers l'EWMQ, un Queue Manager distant comme s'il se trouvait en local. Le système distant peut être un autre Windows, mais également un AS/400, un AIX, Solaris, Linux, …

Sécurisation d'une administration distante

Les risques

Le Queue Manager distant reçoit ses commandes d'administration via le channel SYSTEM.ADMIN.SVRCONN, et ces commandes sont exécutées par le *Command Server* (strmqcsv sur unix/NT).

Le problème est qu'il n'y a, en standard, aucune authentification de la station qui envoie ces commandes. N'importe quel système sur le réseau, pour autant qu'il dispose de quelques

outils et d'un peu de temps, peut envoyer des commandes au Queue Manager distant et prendre la main sur celui-ci.

Ceci n'est pas propre à l'EWMQ. Dès que l'on met en œuvre un outil d'administration MQ distant, il faut démarrer le *Command Server* et on ouvre ainsi la porte aux intrusions.

Avant de mettre en œuvre une administration distance des Queues Managers, quel que soit le produit déployé, il conviendra donc de bien étudier les aspects « sécurité », et de s'assurer que l'on ne risque pas de compromettre les informations transitant dans les queues.

Rôle du paramètre : MCAUSER

Par défaut, les demandes d'administration MQSeries sont exécutées sur le Queue Manager distant avec le même profil (id utilisateur) que celui que vous avez en local.

Si votre id utilisateur sur le système Windows local est par exemple « toto », il faut que le profil « toto » soit connu sur le site distant, et qu'il ait les droits suffisants sur les objets MQSeries. Si les deux systèmes sont dans un domaine Windows, et que votre profil « toto » est de type administrateur ou appartient au groupe « mqm », il n'y aura pas de problème.

Si ce n'est pas le cas (système distant Unix ou AS/400 par exemple) il faut prévoir un paramétrage complémentaire pour que les demandes d'administration MQ arrivant via le channel SVRCONN et le *Command Server* soient prises en compte.

Le paramètre MCAUSER du channel permet de préciser sous quel profil utilisateur les demandes d'administration seront effectuées.

Il y a trois options pour contrôler l'entrée des demandes sur le Queue Manager distant via le MCAUSER :

1. MCAUSER = ‘ ‘ (blanc - valeur par défaut)

   - Les actions d'administration seront effectuées sur le système distant sous le profil utilisé sur le poste de l'EWMQ.

   - Ce profil doit exister sur le système distant et avoir des droits MQ. Le ou les administrateurs utilisant l'EWMQ ont certains droits sur le Queue Manager distant, en fonction des droits MQ attribués à ce profil sur le système distant.

2. MCAUSER = ‘<profil appartenant au groupe mqm>’

   - Les actions d'administration seront effectuées sur le système distant sous le profil spécifié dans le paramètre MCAUSER.

- Ce profil appartenant au groupe « mqm », le ou les administrateurs utilisant l'EWMQ ont tous les droits sur le Queue Manager distant. Ces droits sont donnés via la commande *setmqaut*.

3. MCAUSER = '<profil n'appartenant pas au groupe mqm>'

   - Les actions d'administration seront effectuées sur le système distant sous le profil spécifié dans le paramètre MCAUSER.

   - Ce profil doit exister sur le système distant et avoir des droits MQ. Le ou les administrateurs utilisant l'EWMQ ont certains droits sur le Queue Manager distant, en fonction des droits MQ attribués à ce profil sur le système distant. Ces droits sont donnés via la commande *setmqaut*.

Recommandation

Quelle soit l'option choisie pour le MCAUSER, il y a un risque potentiel d'intrusion dans le système :

- Si le MCAUSR est à blanc, il suffit de lancer une demande d'administration à partir d'un poste où l'on a accès à un profil ayant le nom « mqm » pour administrer totalement le Queue Manager distant.

- Si un profil est spécifié dans le paramètre MCAUSER, n'importe qui, disposant d'un outil d'administration MQ (l'EWMQ ou un autre) pourra se connecter sur le Queue Manager avec les droits du profil indiqué dans MCAUSER.

Il paraît donc prudent, dans un premier temps, de limiter la configuration à la visualisation du statut d'un Queue Manager distant, sans autoriser la modification.

Ce type de configuration peut être obtenu de la façon suivante :

- Création d'un profil, « *mqadmin* » par exemple, sur le système distant. Ce profil n'a pas de droits particuliers sur WebSphere MQ.

- Affectation à ce profil de droits MQ via la commande *setmqaut*, sur les objets dont on veut autoriser l'affichage (plus quelques objets système).

- Création du channel SVRCONN avec MCAUSER = « *mqadmin* ».

Dans un deuxième temps, si l'on souhaite mettre en place une sécurité renforcée (par exemple pour autoriser l'administration totale des Queue Manager à partir d'un EWMQ), il faut prévoir d'authentifier les postes lançant des demandes d'administration. Ceci peut être effectué via les *exit de channel* existants dans WebSphere MQ.

Fin du document