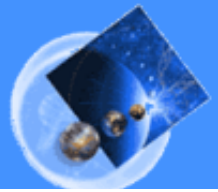
Présentation

Air France – Sécurité IBM MQ

Guide IBM MQ du 8 décembre 2015

F.Beauzon (Air France) - A.Plouviet (Alithya)
G.Trabucco (Air France)

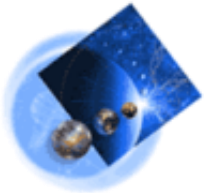
AIRFRANCE



SOMMAIRE

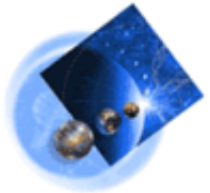
- Objectifs présentation
- Architecture Globale - Air France
- Existant AF - Sécurité IBM MQ
- Etudes en cours
- Questions

3 Objectifs présentation



- ✓ Exposer la sécurité IBM MQ au sein d'Air France
- ✓ Aborder nos études et nos recherches en cours
- ✓ Echange mutuel à travers vos questions et retours d'expériences

4 Architecture Globale – AF



M.Q.O.M

MQ :

- MQ V7.1 - multi Queue Manager/Serveurs

Systeme :

- Linux (Red-Hat)
- Haute dispo : VCS - PRA
- Sécurité : SAR – ssh/scp - droits fichiers MQ limités - Etanchéité des env.

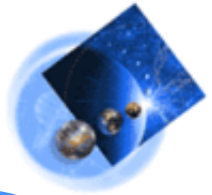
Supervision - Tracabilité

- BMC TrueSight Middleware Monitor / HP-OVO
- Archivage msg MQ

RZO :

- Interne / zones cloisonnées / dédié au monde Aérien / VPN

5 Existant AF: Sécurité des Objets IBM MQ



Règles générales sur les Objets IBM MQ :

- **OAM** (GroupID appli « no such schell »)
- SVRCONN : MCAUSER
- SYSTEM.DEF.SVRCONN (« nobody »)
- IBM MQ SSL/TLS
- Queues Alias

Spécificités Applications Internes SI AF

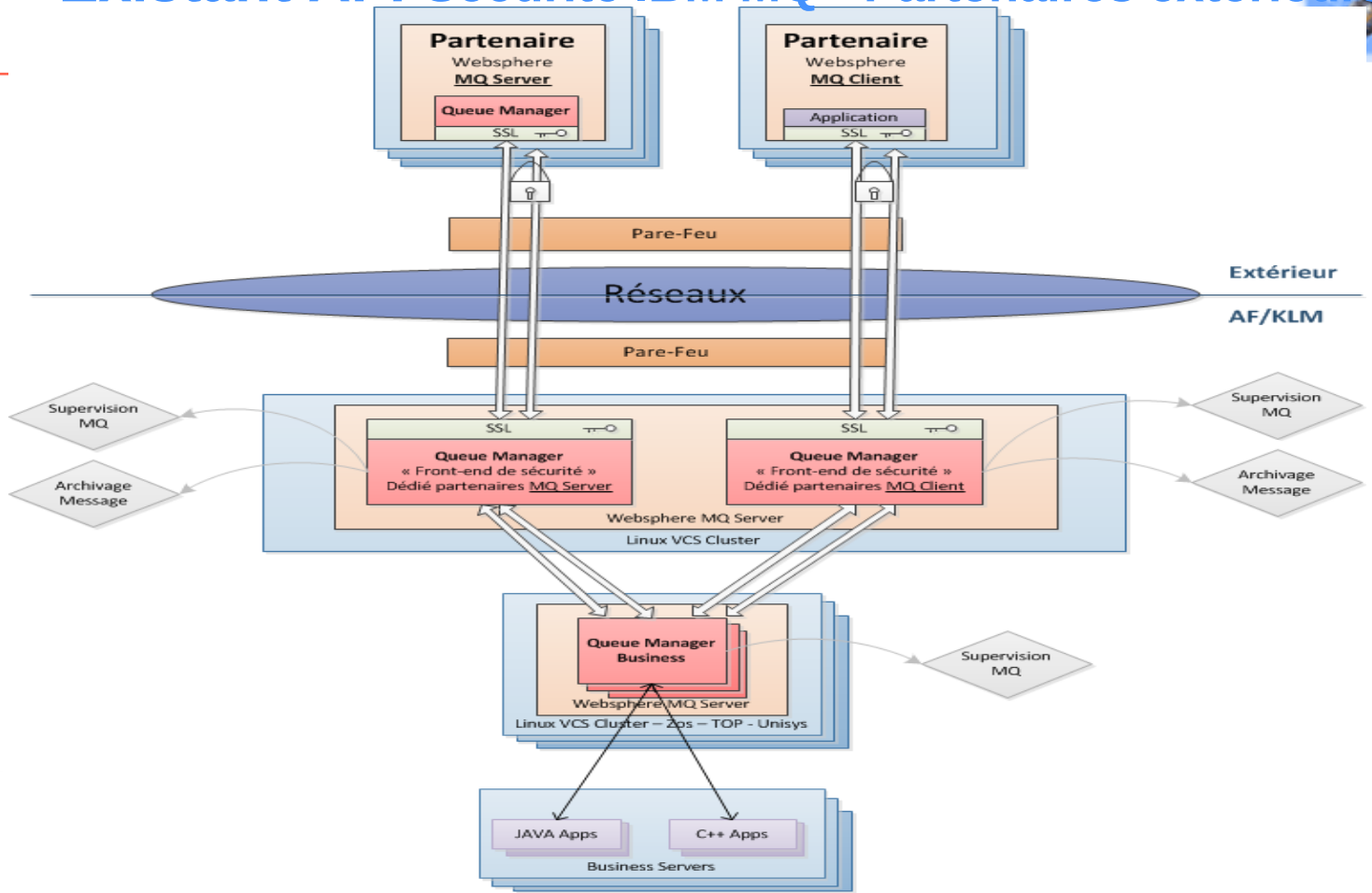
- Mode client (Java/JMS via bindings et C++ via API)
- Serveurs business selon domaine fonctionnel
- QM Zone cloisonné si nécessaire

6 Existant AF: Sécurité IBM MQ - Partenaires extérieurs

- QMs dit « Front-end » de sécurité => Pas d'accès direct QM interne/externe
- Adresses « Nattées » (Firewall)
- Canaux :
  - MCAUSER (SVRCONN/RCVR)
  - IBM MQ SSL obligatoire
  - Dédiés type de flux

- Paramètres sécurité QM:
  - OCSPCheckExtensions=NO
  - SSLPIPS(NO), CHLAUTH(DISABLED)

7 Existant AF: Sécurité IBM MQ - Partenaires extérieurs



8 Existant AF: Niveaux de sécurité IBM MQ
→ Canaux SDR/RCVR (mode Serveur)

Niveau de Sécurité Canaux Servers (SDR/RCVR)	Certificat SSL QM	MCAUSER (RCVR)	SSLCIPH	SSLPEER
Niveau 0 Sans sécurité	-	-	-	-
Niveau 1 Avec OAM	-	GroupID	-	-
Niveau 2 Authentification	✓	GroupID	NULL_SHA*	-
Niveau 3 Auth + DN	✓	GroupID	NULL_SHA*	DN du certif. QM distant
Niveau 4 Auth + Chiffrement	✓	GroupID	TLS_RSA_WITH_AES_256_CBC_SHA TRIPLE_DES_SHA_US*	-
Niveau 5 Auth + Chiffrement + DN	✓	GroupID	TLS_RSA_WITH_AES_256_CBC_SHA TRIPLE_DES_SHA_US*	DN du certif. QM distant

** En cours de remplacement par CipherSpec TLS ou non utilisé*

9 Existant AF: Niveaux de sécurité IBM MQ
→ Canaux SVRCONN (mode Client)

Niveau de Sécurité Canal Client (SVRCONN)	Certificat application	MCAUSER	SSLCAUTH	SSLCIPH	SSLPEER
Niveau 0 Sans sécurité	-	-	REQUIRED	-	-
Niveau 1 Avec OAM	-	GroupID (APPLI)	REQUIRED (défaut)	-	-
Niveau 2.1 Authentification « partielle»	-	GroupID	OPTIONAL	NULL_SHA*	-
Niveau 2.2 Auth + Certif Appli	✓	GroupID	REQUIRED	NULL_SHA*	-
Niveau 2.3 Auth + Certif Appli + DN	✓	GroupID	REQUIRED	NULL_SHA*	Channel : DN certif Appli Bindings Appli : DN Qmgr
Niveau 3.1 Auth «partielle» + Chiffrement	-	GroupID	OPTIONAL	TLS_RSA_WITH_AES_256_CBC_SHA TRIPLE_DES_SHA_US*	
Niveau 3.2 Auth + Chiff + Certif Appli	✓	GroupID	REQUIRED	TLS_RSA_WITH_AES_256_CBC_SHA TRIPLE_DES_SHA_US*	
Niveau 3.3 **Auth + Chiff+ Certif Appli + DN**	✓	GroupID	REQUIRED	TLS_RSA_WITH_AES_256_CBC_SHA TRIPLE_DES_SHA_US*	Channel : DN certif Appli Bindings Appli : DN Qmgr

** En cours de remplacement par CipherSpec TLS ou non utilisé*

10 Existant AF: Gestion des certificats IBM MQ SSL/TLS (1)

Contrainte : Avant MQ V8, 1 seul certificat QM avec le label **ibmwebspheremq<qmgr>**

Besoin :

- Anticiper les changements de certificat de QM
- Industrialisation
- Sauvegarde/Restauration rapides

Solution : Pour chaque QM, 2 types de magasins de certificats

⇒ Actif : utilisée par le QM (SSLKEYR)

⇒ Non actif : copie en phase de préparation

11 Existant AF: Gestion des certificats IBM MQ SSL/TLS (2)

Outil d'administration SSL
(Distant, en mode commande ou interactif)

Gestion des magasins
- Création/Sauvegarde/Restauration
- Copie/Refresh magasin actif <=> non actif (mesa)

Gestion des certificats :
- Actions/Consultation des certificats
- Certificats périmés

Gestion des canaux :
- Activer/désactiver SSL
- Informations/statut

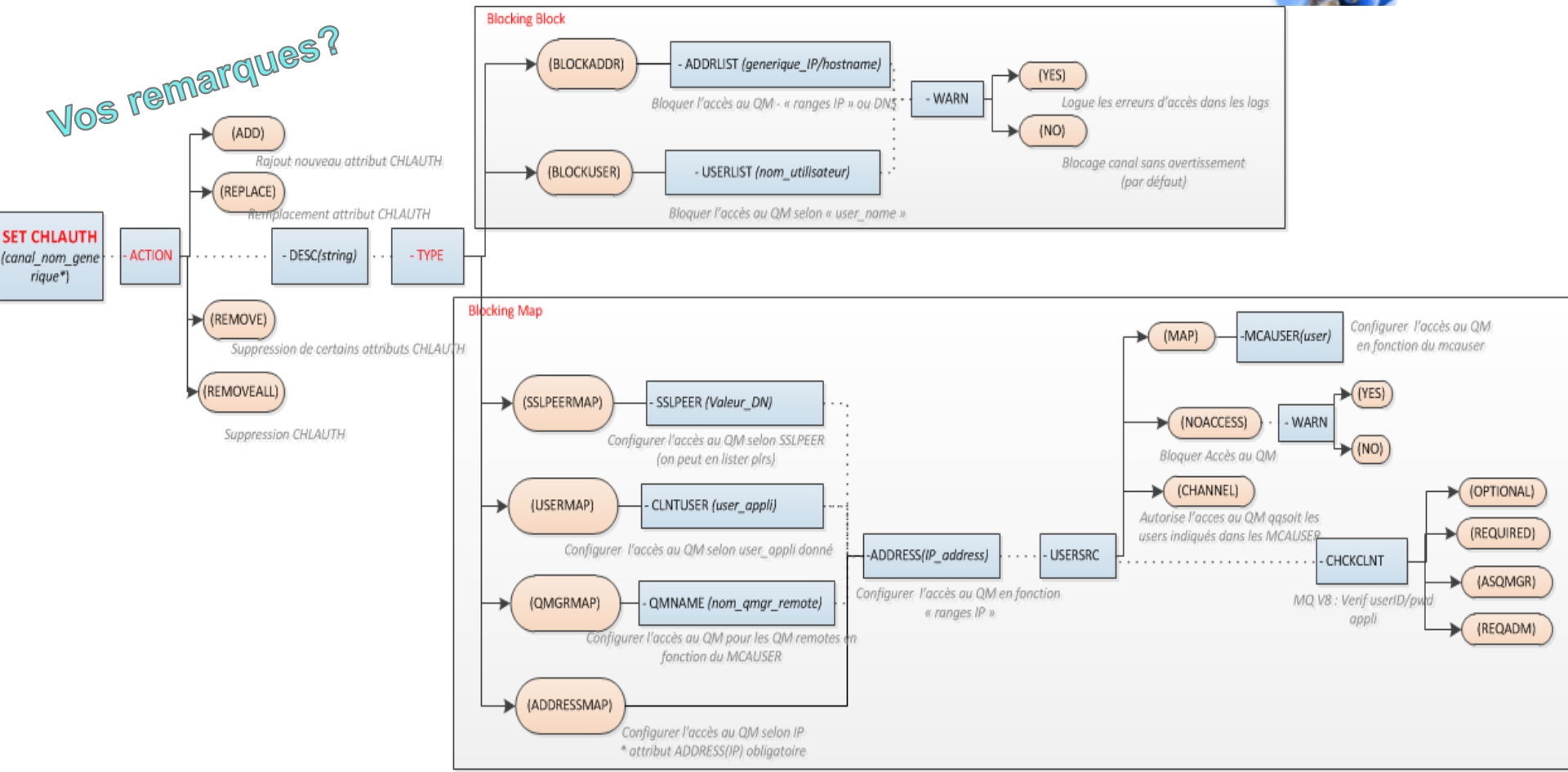
12 Etudes en cours: Connexion Authentification

Votre avis ?

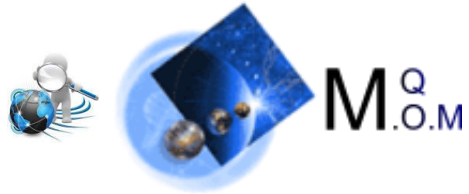
Authentification connexion	Paramètres MQ	Questions
Niveau Application UserID/pwd	1) Code applicatif 2) Channel Security Exit (mqccred) + PasswordProtection dans qm.ini ou mqclient.ini	**Q1 : Moins secure que SSL/TLS ou OAM?** **Q2 : utilisez-vous channel security exit ?**
Type 1 : Niveau QM UserID/pwd => **Par l'OS**	**ALTER QMGR CONNAUTH(<*Objet_authinfo*>)** **DEFINE AUTHINFO(<*Objet_authinfo*>)** **AUTHTYPE(IDPWOS)**	**AF : OAM selon MCAUSER** Rajout des droits sur le GroupID. UserID définit dans /etc/passwd en /nosuchshell **sans password** **SAR** : matricule personnel (selon groupe service AF) changement des pwd régulièrement. **sudo su - mqm** => **Quid SAR ?**
Type 2 : **Niveau QM** UserID/pwd => **Par LDAP** (User Repositories)	**ALTER QMGR CONNAUTH(<*Objet_authinfo*>)** **DEFINE AUTHINFO(*Objet_authinfo*)** **AUTHTYPE(IDPWLDAP)**	

13 Etudes en cours: Canal Authentification

Vos remarques?



14 Nos prochaines études



1) Mise en place d'un Anti-virus (Recommandations de notre sécurité)

→ Et vous ?

2) Password magasin de certificat en mode client Java-JMS : "en clair" dans le code applicatif

→ Comment se protéger? Utilisez-vous "keystore.conf" ?

3) Erreurs IBM MQ SSL /TLS: manque de visibilité coté MQ Serveur.

→ Avez-vous rencontré ces difficultées ? Résolution ?

4) Gestion des profils en fonction des niveaux d'exploitation

« runmqsc » (local/remote) pour les users hors mqm group avec les droits OAM

→ Le gérez vous ?

15 Questions

16 Annexe 1 : Principes de sécurité

- **Confidentialité** : Protection des données sensibles contre la divulgation ou l'interception non autorisée sous forme intelligible
- **Intégrité** : Protection de la précision et de l'intégralité des données et des logiciels
- **Disponibilité** : Garantie de l'accessibilité des données en temps utile
- **Traçabilité** : Garantie d'un moyen permettant de retrouver rétrospectivement les états successifs (modifications) des données et d'identifier les auteurs de ces modifications

17 Annexe 2: Connexion Authentification

Types Authentification connection	Descriptif / Rem	Paramètres MQ
Type 1: Par l'application (MQCSP password protection)	Auth. APPLI UserID/PWD	1) Lors du MQCONNX, l'appli peut fournir UserID & password (modif code appli.) => vérification OAM 2) Autre possibilité : mqccred (channel security exit => pas de modif dans code appli) Avec PasswordProtection dans qm.ini ou mqclient.ini
Type 2 : Par l'OS AUTHTYPE(**IDPWOS**)	**Authentification UserID/PWD par OS** Un seul AUTHINFO par QM refresh security type(connauth) => dynamique	**QMGR, Attribut: CONNAUTH(nom_objet_authinfo)** Objet **AUTHINFO,** attributs : 1) AUTHTYPE(**IDPWOS**) => verif user/pwd OS 2) Cnx locale: CHCKLOCL pas à AF 3) Cnx Client: CHCKCLNT 4)ADOPTCTX
Type 3 : **Par LDAP** (User Repositories) AUTHTYPE(**IDPWLDAP**)	**Auth + chiff.(option) UserID/PWD par LDAP** Un seul AUTHINFO par QM refresh security type(connauth) => dynamique	**QMGR, Attribut: CONNAUTH(nom_objet_authinfo)** Objet **AUTHINFO** avec attributs : 1) AUTHTYPE(**IDPWLDAP**) => verif user/pwd via LDAP 2) CONNAME(serveur_ldap) 3) LDAPUSER 4) LDAPPWD