© Demey Consulting, 2001-2024 - Reproduction interdite



# IBM MQ
# Evolutions TLS 2024

Une production : Demey Consulting

Version 1.00 - Octobre 2024

© Demey Consulting, 2001-2024 - Reproduction interdite



# IBM MQ 9.3 : Support des magasins PKCS12

Remplaçant potentiel des magasins en format CMS (.kbd) et JKS pour :

- les QM
- Les clients MQ C
- Les clients MQ Java
- MQIPT
- MQ Explorer
- MFT
- Native HA
- JWT

© Demey Consulting, 2024

© Demey Consulting, 2001-2024 - Reproduction interdite



# Principales différences

- Magasin PKCS 12 :
  - Pas de fichier stash
  - CMS : format propriétaire IBM
  - PKCS12 : standard du marché
- Pour un Queue Manager :
  - Avant MQ 9.3 : nom du magasin cms sans l'extension
  - A partir de MQ 9.3
    - nom du magasin sans l'extension : format cms
    - nom du magasin avec extension .kdb : format cms
    - nom du magasin avec extension .p12 : format pkcs12

© Demey Consulting, 2001-2024 - Reproduction interdite



# Le problème du mot de passe

- Format cms : fichier "de dissimulation" .sth
  - Contient le mot de passe en format crypté (algo propriétaire IBM)
  - Algo change régulièrement
- Format PKCS12
  - Attribut KEYRPWD pour un QM

    Variable MQKEYRPWD pour un client

    SSLKeyRepositoryPassword dans le mqclient.ini

    → le mot de passe est fourni en clair

© Demey Consulting, 2001-2024 - Reproduction interdite



# Solution : Chiffrement du mot de passe

- Queue Manager : Chiffré automatique lors de la mise à jour de KEYRPWD
- Client MQ : runmqicred pour chiffrer le mot de passe

- Chiffrement AES-128 → nécessite une clé
  - Par défaut : clé identique pour toutes les installations

- Fourniture d'une clé spécifique à l'installation :
  - Dans le paramètre INITKEY si Queue Manager
  - Dans un fichier si client MQ
    - Variable d'environnement : MQS_MQI_KEYFILE
    - MQIInitialKeyFile dans mqclient.ini

© Demey Consulting, 2001-2024 - Reproduction interdite



# Did you know IBM MQ supports PKCS#12 keystores?

By Rob Parker posted Tue August 13, 2024 07:00 AM

https://community.ibm.com/community/user/blogs/robert-parker1

© Demey Consulting, 2001-2024 - Reproduction interdite



# IBM MQ 9.4 et TLS

(Linux, Unix & Windows)

- Nouvelles commandes
  - runmqckm est remplacé par runmqktool
  - strmqikm (interface graphique) est supprimé
- runmqktool :
  - pas de support des fichiers stash
  - pas de support des fichiers CMS
  - nécessite IBM MQ Java runtime
- runmqakm reste disponible et peut :
  - gérer des fichiers CMS et PKCS12
  - gérer des fichiers stash

© Demey Consulting, 2001-2024 - Reproduction interdite



# Autres points (9.4.0)

- TLS Certificate bypass option
  - Permet à un client MQ de ne pas vérifier le certificat envoyé par le serveur
  - Nouvelle valeur pour Certificate validation policy : NONE
    - SET MQCERTVPOL=NONE
    - CertificateValPolicy=NONE

https://www.ibm.com/docs/en/ibm-mq/9.4?topic=mq-configuring-certificate-validation-policies-in

© Demey Consulting, 2001-2024 - Reproduction interdite



# Autres points 9.4.1

- Expiration Certificate Monitor
  - Commande dspmqcert
- Désactivation de cipherspecs :
  - Tous ceux commençant par TLS_RSA_WITH_
  - Ré-activables si besoin
  - Migration vers ECDHE_RSA_ recommandée

© Demey Consulting, 2001-2024 - Reproduction interdite



# Recommandations

- Migrer progressivement vers des magasins PKCS12
  - Sécurité
  - Risque de déprécation du format CMS
  - Outils standards pour gestion des magasins
- Mettre à jour les cipherspecs utilisés
  - Passer de TLS_RSA_WITH_ à ECDHE_RSA_ (par exemple)
  - AVANT le passage en MQ 9.4
- Migrer vers TLS 1.3
  - Préparer le « Quantum Safe »

© Demey Consulting, 2001-2024 - Reproduction interdite



# *Merci de votre attention*

© Demey Consulting, 2001-2024 - Reproduction interdite



# La formation avec Demey Consulting

- Un organisme de formation déclaré et Datadocké"
- Un catalogue de modules sur WebSphere Application Server et IBM MQ
- Plus de 50 modules MQ disponibles (1500 slides)
- Des supports de cours totalement francisés et au dernier niveau technique (MQ version 9.4.1)
- Des travaux pratiques sur Windows, Linux et iSeries avec les corrigés
- Des filières prédéfinies de 2 à 5 jours, ou à la carte.

https://demey-consulting.fr/formationMQ