IBM MQ V9.3 アップデート・セミナー

第2章：新機能・変更点

6. その他（共通・分散）

内容

- ライセンス / インストール
- Administration
- セキュリティ
- アプリケーション
- Advanced関連
- メッセージの追加・変更・削除
- Deprecated / Stabilized / Removed

ライセンス / インストール

ライセンス / インストール

ALW
V9.3.0/V9.2.2/
V9.2.0.3

- Advanced版の開発･テスト用ライセンス（Non-Protuctiveライセンス）の追加
  - ◆ setmqinst -lオプションにて [nonprod]を指定

Windows
V9.3.0/ V9.2.1

- 「ライセンス資格の確認」画面の追加
  - ◆ インストーラーで下記のコンポーネントを選択する際に、「Advanceライセンスが必要」の警告画面を表示
    - Advancedライセンスが必要な以下のコンポーネントを誤ってインストールするリスクを低減
      - MQ Telemetry Service
      - Advanced Message Security
      - Managed File Transfer Service
  - ◆ Launchpadパネルに追加

IBM i
V9.3.0

- MQ for IBM iにて、ライセンス設定のため、以下のコマンドの機能拡張
  - ◆ dspmqinst
    - インストール済み環境の表示コマンド
    - MQ for IBM i ではオプションは使用不可
  - ◆ setmqinst
    - インストール済み環境の設定変更
    - -l オプションにて、エンタイトルメントに”hareplica”または”nonprod”の指定が可能

ライセンス / インストール

Linux
V9.3.0 /V9.2.1

- アップグレード手順の簡素化
  - ◆ 前バージョンの製品のアンインストールを行わずに、MQのアップグレードが可能
  - ◆ 前提
    - アップグレード前のバージョンがMQ V9.2.0以降
    - Fix Packが未適用であること
      - V,R,M,FのFレベルが0であること
      - 例
        - V9.2.0.0 →アップグレード可能
        - V9.2.0.5 →アップグレード不可、前バージョンのアンインストールを行った後にマイグレーションを行う
- アップグレード用コマンド

種類	サンプルコマンド	プラットフォーム
rpmコマンド	rpm -Uvh MQSeries*	Linux
yumコマンド	yum -y upgrade MQSeries*	Red Hat
dpkgコマンド	dpkg -i *packageName*	Ubuntu
aptコマンド	apt-get upgrade "ibmmq-*"	Ubuntu

ライセンス / インストール

Multi.
V9.3.0 /V9.2.4

- MQコード署名サポート
  - ◆ IBMサイトからのダウンロードファイル、導入メディアに電子署名を付与
  - ◆ ダウンロード・ファイル、導入メディア
    - ● ダウンロード・メディアの署名チェックのための追加パッケージをFix Centralからダウンロード
      - 追加パッケージには署名とパブリックキーが含まれる
      - 入手先： https://ibm.biz/mq93signatures

ライセンス / インストール

Multi.
V9.3.0 /V9.2.4

◆ メディアタイプと検証方法

メディア種類	検証キーなど	チェック方法
*.zip	組込デジタル署名付きで配布 JDKによる検証	（コマンド例） jarsigner -certs -verify 9.2.4.0-IBM-MQC-Redist-Java.zip （応答例） jar verified
*.tar.gz	IBMによる署名済みで配布 デジタル署名を追加ダウンロード opensslによる検証	（コマンド例） openssl dgst -sha256 -verify ibm_mq_public.pem -signature 9.2.4.0-IBM-MQC-Redist-LinuxX64.tar.gz.sig 9.2.4.0-IBM-MQC-Redist-LinuxX64.tar.gz （応答例） Verified OK
*.rpm	デジタル署名付きで配布 IBM MQ 公開署名 gpg キーを取得し、rpm にインストール rpmコマンドによる検証	（コマンド例） # rpm -Kv MQSeriesRuntime-9.2.4-0.x86_64.rpm （応答例） MQSeriesRuntime-9.2.4-0.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID 0209b828: OK Header SHA1 digest: OK V3 RSA/SHA256 Signature, key ID 0209b828: OK MD5 digest: OK
*.deb	組み込みデジタル署名で署名済み IBM MQ 公開署名 gpg キーとdebsigsパッケージをインストール debsigs-verifyユーティリティで検証	KnowlegeCenterの記述を参照 https://www.ibm.com/docs/ja/ibm-mq/9.3?topic=overview-mq-code-signatures

ライセンス / インストール

Windows/Linux
V9.3.0 /V9.2.4

- IBM MQエクスプローラーの配布方法の変更
  - ◆ Fix Centralで配布
  - ◆ 製品の導入パッケージからは削除
    - FixCentralから、別途ダウンロード・インストールを行う

Java
V9.2.2 /V9.2.0.2

- JMSAdminツール導入の簡素化
  - ◆ 自己解凍型JARファイル： *version*-IBM-MQ-Install-Java-All.jarが JMSadminツール関連のファイルを含むように更新
    - 以下のファイルを含むよう変更された
      - JMSAdmin.bat （JMSAdminツール起動用、Windows版）
      - JMSAdminスクリプト（JMSAdminツール起動用、Linux/Unix用）
      - JMSAdminツールのサンプル構成ファイル（(JMSAdmin.config)

※ MQ V9.3以降はJakarta Messagingのページを参照

Administration

Multi.
V9.3.0 /V9.2.3

リモート接続可能なDLQハンドラーの提供

◆ DLQハンドラーをMQクライアント・パッケージにも提供

- サーバーパッケージには従来から提供
- DLQハンドラーのサンプル・コード(/opt/mqm/samp/dlq配下)をMQクライアント接続対応に更新

◆ runmqdlqコマンドに-cオプション指定でクライアント接続を行う

- 接続先は以下のいずれかの方法で付与
  - MQSERVER環境変数
  - MQCHLLIB/MQCHLTAB環境変数

ALW
V9.3.0 /V9.2.1

DELETEコマンドにIGNSTATEオプションを追加

◆ 存在しない(≒削除済みの)MQオブジェクトの削除を試みたとき、コマンドををエラーにする/しないを制御可能

- IGNSTATE(NO)[デフォルト、現行と同じ動作]
  - 「該当MQオブジェクトなし」のエラーを返却

```
delete ql(QL01) ignstate(no)
     8 : delete ql(QL01) ignstate(no)
AMQ8147E: IBM MQ object QL01 not found.
```

- IGNSTATE(YES)
  - 「該当MQオブジェクトを削除しました」の正常応答を返却

```
delete ql(QL01) ignstate(yes)
     9 : delete ql(QL01) ignstate(yes)
AMQ8007I: IBM MQ queue deleted.
```

Multi.
V9.3.0 /V9.2.1

- キュー・マネージャー起動時のMQSC自動構成機能の変更
  - qm.iniのAutoConfigスタンザ-MQSCConfigに指定されたすべてのMQSCコマンドが実行された後、アプリケーションからの接続が可能となるよう、動作の変更

Multi.
V9.3.0 /V9.2.2

- リモート接続時のrunmqscコマンド変更
  - -w：WaitTimeの指定
    - V9.3.0/V9.2.2より、コマンドメッセージの有効期限として設定
    - コマンド応答メッセージには、有効期限の残りがセットされる
  - コマンド応答を受け取るSYSTEM.MQSC.REPLY.QUEUEのMAXDEPTHを99999999に変更
    - 以前は30000

共通
V9.3.0 /V9.2.2/
V9.2.0.2

- DISPLAY CHSTATUS・Inquire Channel Statusコマンドの戻りの変更
  - 以下の属性が999999999でラップ（0 に戻る）
    - DISPLAY CHSTATUS: BYTSSENT / BYTSRCVD
    - Inquire Channel Status : BytesSent / BytesReceived

AIX
V9.3.0 /V9.2.1

- zlibNX 圧縮ライブラリーのサポート
  - チャネルのデータ圧縮にハードウェアアクセラレーター（zlibNX library ）を使用可能
    - 環境変数：AMQ_USE_ZLIBNXの追加
    - チャネル定義のCOMPRESS属性にてZLIBFASTまたはZLIBHIGHを指定する場合に有効
    - AIX 7.2 TL 4 Expansion Pack以降で使用可能

Multi.
V9.3.0

- MQIPT関連
  - ネットワークトレースの量を指定可能
  - mqipt.confのTraceUserDataプロパティにて指定
    - 指定可能値
      - 0：トレース取得なし
      - all：全量トレース
      - バイト数：取得する容量を指定。１５以上

Multi.
V9.3.0 /V9.2.4 /
V9.2.0.3

- runmqrasコマンドの変更
  - -noqmdataオプション
    - キュー・マネージャーレベルのデータを収集しないオプションの追加

■ キュー会計/MQI会計メッセージにクライアント接続時のConnName情報が追加

Multi.
V9.3.0 /V9.2.4

フィールド	フィールドID	データ型	説明
ConnName	MQCACH_CONNECTION_NAME	MQCFST	クライアント接続のCONNAME

- 会計/統計メッセージの詳細は以下を参照
  - Accounting and statistics messages
    - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=network-accounting-statistics-messages
  - Queue accounting message data
    - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=reference-queue-accounting-message-data
  - MQI accounting message data
    - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=reference-mqi-accounting-message-data

■ LDAP接続時のチューニングパラメータ追加

Multi.
V9.3.0 /V9.2.4 /
V9.2.0.3

◆ qm.iniのTuningParameterスタンザに追加

- OAMLdapConnectTimeout=*maximum time*（秒）
  - LDAP接続までの最大待ち時間
- OAMLdapQueryTimeLimit=*maximum time*（秒）
  - LDAP接続時の最大応答待ち時間

- OCSP接続時のチューニングパラメータ変更
  - qm.ini、mqclient.iniのSSLスタンザ
    - OCSPTimeout= *number*に0を設定した場合には、デフォルトの30(秒）が使用されるよう変更

Multi.
V9.3.0/V9.2.3/
V9.2.0.2

セキュリティ

非OSユーザーに対する認可

AL
V9.3.0 /V9.2.1

- 非OSユーザーへの権限付与
  - ◆ 認可モデルが単純化
    - 主にコンテナ環境のMQ向け
      - ローカルOS環境においてユーザーが管理されていない環境において有効
  - ◆ UserExternalオプションの追加
    - OS/LDAPに存在しないユーザーに権限付与が可能
    - ユーザー名は12文字まで
      - 権限の付与とチェックに使用可能
      - ユーザー名に使用可能な文字は、MQオブジェクトに使用可能な文字と同等
- UserExternalの指定方法
  - ◆ キュー・マネージャー作成時、oaオプションで指定

```
crtmqm -oa UserExternal QM01
```

  - ◆ qm.iniのサービススタンザで指定

```
Service:
   Name=AuthorizationService
   EntryPoints=14
   SecurityPolicy=UserExternal
```

非セキュア通信の可否設定

Multi.
V9.3.0 /V9.2.1

- 非セキュアな通信の排除が可能
  - qm.iniのTCPスタンザに指定
  - パラメータ：SecureCommsOnly
  - 設定
    - SecureCommsOnly＝NO|N|FALSE|F　（デフォルト値）
      - 非TLSチャネル接続が可能
      - キュー・マネージャー起動時にWarningメッセージが出力

```
AMQ9722W: Plain text communication is enabled.
```

    - SecureCommsOnly=YES|Y|TRUE|T
      - TLSチャネルの接続のみ可能
      - キュー・マネージャー起動時にInformationメッセージが出力

```
AMQ9723I: Secure communication only is enabled.
```

      - 非TLSチャネル接続起動時にエラー出力

```
AMQ9278E: TCP/IP channel 'QM930A.QMNHA
' suppressed as it does not use
a secure communications protocol.
```

TLS関連

共通 V9.3.0
Dist.
V9.3.0/ V9.2.4

- TLS 1.3をサポートするJREをMQで提供
  - V9.2ではJREは別パッケージで提供されていた

ALW
V9.3.0

- PKCS#12 鍵リポジトリーのサポート
  - 鍵リポジトリーのタイプにPKCS#12を指定して鍵リポジトリーの作成が可能
    - 拡張子は.p12で作成される

```
runmqakm -keydb -create -db filename -pw password -type cms | pkcs12
```

  - 鍵リポジトリーの指定方法の変更
    - 鍵リポジトリーファイル名フルパス（拡張子付き）で指定可能
      - キュー・マネージャーのSSLKEYR属性

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey.p12')
```

      - MQクライアント（Linux・AIX）の例

```
export MQSSLKEYR=/var/mqm/ssl/key.p12
```

    - 従来の指定（拡張子なし）の場合、
      - 拡張子なしのファイルを検索
        - 拡張子なしのファイルが存在しない場合は、.kdbの拡張子が付いたファイルを検索

ALW.
V9.3.0/V9.2.5

■ 鍵リポジトリーの変更を検知するタイミングの制御

◆ mqclient.iniのSSLスタンザ：EnvironmentScopeに指定

- PROCESS（デフォルト）：
  - 全TLSセッションが終了するまで検知しない
  - TSLセッションを開始したプロセスが終了した後、次のTLSセッション開始後に変更を反映
- CONNECTION：
  - 新規のTLSセッションから変更を反映

  ＊当該設定により追加のCPU/メモリーを消費する

- Cクライアントおよび非管理コードの.NETクライアントにおいて有効

パスワード保護機能

- MQの特定の機能を使用する際にパスワードを提供する場合がある
  - パスワードを直接提供または特定機能が使用する構成ファイルに提供
  - MQ V9.2.0以降、構成ファイル内のパスワード保護機能が実装
    - MFT、Saleforceブリッジ、Blockchainブリッジなど
    - V9.2. XおよびV9.3.0でパスワード保護機能が強化された

- パスワード保護機能の用語について
  - イニシャル・キー（Initial Key）
    - ユーザー側で指定する暗号化キー
    - 構成ファイルを使用する場合には、1行で指定
      - キーの長さの制約はないが、16文字以上を推奨（最低：1文字）
  - MQ提供のキー（Default Initial Key）
    - イニシャル・キーを指定しない場合に使用される、MQが内部で保持するイニシャル・キー

注意：コンポーネント毎に提供されているユーティリティでパスワード保護・暗号化を行うこと
- あるコンポーネントで使用するために生成したエンコード・パスワード・ストリングを、別のコンポーネントの構成ファイルにコピーして使用することは不可

パスワード保護機能の強化

Multi.
V9.3.0

■ 鍵リポジトリーのパスワードの指定と保護設定

◆ V9.2までは、stash fileを使用

- V9.3でもstash fileを継続使用可能

◆ キュー・マネージャーの場合

- 鍵リポジトリーのパスワード指定
  - キュー・マネージャーのKEYRPWD属性で指定
    - 鍵リポジトリーのパスワードを設定
    - MQによってパスワードが暗号化された後に保管
    - DISPLAY QMGR KEYRPWDでは***でマスクされる

- 暗号化キーをユーザーが指定する場合
  - キュー・マネージャーのINITKEY属性にイニシャル・キーを設定後
    - 設定後にKEYRPWD属性を更新
    - DISPLAY QMGRコマンドではINITKEY属性は****で表示される
    - KEYPWD属性更新後、INITKEY属性は変更不可

パスワード保護機能の強化

Multi.
V9.3.0

◆ MQクライアント

- 鍵リポジトリーのパスワード指定
  - 以下のいずれかでパスワードを指定
    - ① MQSCO構造体のVersion6で追加されたフィールドを使用
      - KeyRepoPasswordPtr
      - KeyRepoPasswordOffset
      - KeyRepoPasswordLength
    - ② MQKEYRPWD環境変数で指定
    - ③ mqclient.ini のSSLKeyRepositoryPassword属性に指定

mqclient.iniの例

```
SSL:
   SSLKeyRepositoryPassword=passw0rd
```

- MQクライアントでのパスワード保護
  - 上記手順にて鍵リポジトリーにパスワードを指定する場合、以下の方法で事前にパスワードを暗号化すること
  - MQクライアントパスワード保護コマンド：runmqicredコマンドにイニシャル・キーを付与して実行
    - コマンドの’-sf‘引数にイニシャル・キーを記述したファイルを指定
    - MQS_MQI_KEYFILE環境変数にイニシャル・キーを記述したファイルを指定
    - 未指定の場合はMQ提供のキーで暗号化される
  - コマンド実行結果として暗号化後の文字列を返す
  - 暗号化されたパスワードを鍵リポジトリーのパスワードとして、上記①～③に指定

パスワード保護機能の強化

Multi.
V9.3.0

◆ MQクライアントアプリケーション実行時

- キーを付与してパスワードを暗号化した場合は、アプリケーション実行時に暗号化に使用したキーを付与する

  - アプリケーションへのキー付与方法は以下のいずれか

    ① MQCSP構造体の以下のフィールドにキーを指定
    - InitialKeyPtr
    - InitialKeyOffset
    - InitialKeyLength

    ② MQS_MQI_KEYFILE環境変数にイニシャル・キーを記述したファイルを指定

    ③ mqclient.iniのセキュリティスタンザ
    - MQIInitialKeyFileにイニシャル・キーを記述したファイルを指定

パスワード保護機能の強化

ALW
V9.3.0/ V9.2.3

- 暗号化ハードウェアを使用するMQクライアントのパスワード保護機能の強化
  - ◆ PKCS #11 暗号化ハードウェアにTLS 通信で使用する秘密鍵と証明書を保管するように MQ クライアントを構成可能
    - mqclient.iniのSSLスタンザ CryptoHardwareに暗号化ハードウェア情報を記載
      - CryptoHardware属性に指定するパスワードをrunp11credコマンドで保護可能
  - ◆ パスワード保護
    - runp11cred：PKCS #11 暗号化ハードウェア・パスワードの保護コマンドを使用
    - runp11credコマンドを実行し、パスワードを入力
      - 暗号化された文字列が返却される
    - イニシャル・キーは以下の方法で付与可能
      - コマンドの'-sf'引数にイニシャル・キーを記述したファイルを指定
      - MQS_SSLCRYP_KEYFILE 環境変数にイニシャル・キーを記述したファイルを指定
      - 未指定の場合はMQ提供のキーで暗号化される
    - 暗号化されたパスワードをSSL.CryptoHardwareに指定

```
$ runp11cred
5724-H72 (C) Copyright IBM Corp. 1994, 2022.
パスワードを入力してください:
******
資格情報はデフォルトの暗号鍵を使用して暗号化されます。
保管される資格情報をより安全に保護するには、
カスタムの強い暗号鍵を使用してください。
<P11>!2!RrVWJqxxGIya6GEBUNFlnPb12WdD7PeEBBeaugBvqKo=!73Eo1yt99a2pSe3KnxRPFQ==
```

  - ◆ MQクライアントアプリケーション実行時
    - パスワードを暗号化した場合は、アプリケーション実行時に暗号化に使用したキーを付与する
      - MQS_SSLCRYP_KEYFIL環境変数にイニシャル・キーを記述したファイルを指定

パスワード保護機能の強化

IBM i
V9.3.0/ V9.2.3

- CHGMQMコマンドの変更
  - SSLKEYRPWDに指定したパスワードが、イニシャル・キー（INITKEY）により暗号化されるよう変更
  - SSLKEYRに指定する際は鍵リポジトリーのフルパス（拡張子付き）で設定

OutboundSNI

Multi.
V9.3.0/ V9.2.1

- SSLスタンザにてTLSのOutboundSNI属性追加
  - ◆ 対象：qm.iniおよびmqclient.ini
    - CHANNEL:
      - TLSクライアントはTLS 接続の開始時にSNIを接続先キュー・マネージャーの チャネル名に設定
      - 接続先キュー・マネージャーにチャネルの証明書（個別）を送付するように要求
    - HOSTNAME:
      - TLSクライアントはTLS接続開始時にSNIをホスト名に設定
      - 接続先キュー・マネージャーにキュー・マネージャー証明書（デフォルト）を送付するように要求
  - ◆ AllowOutboundSNIはV9.2.1以降は非推奨
    - 「AllowOutboundSNI=YES」 =「OutboundSNI=CHANNEL」
    - 「AllowOutboundSNI=NO」 =「OutboundSNI=HOSTNAME」

OutboundSNI

Multi.
V9.3.0/ V9.2.4

- 管理コード.NETおよびXMS.NETでSNIの指定が可能
  - ◆ V9.2.3以前は非管理コード.NETでのみ指定可能
  - ◆ 管理コード.NET
    - mqclient.ini のSSLスタンザにてOutboooundSNI指定が可能
      - CHANNEL:
        - TLSクライアントはTLS 接続の開始時にSNIを接続先キュー・マネージャーの チャネル名に設定
        - 接続先キュー・マネージャーにチャネルの証明書（個別）を送付するように要求
      - HOSTNAME:
        - TLSクライアントはTLS接続開始時にSNIをホスト名に設定
        - 接続先キュー・マネージャーにキュー・マネージャー証明書（デフォルト）を送付するように要求
  - ◆ XMS
    - MQOUTBOUND_SNI環境変数
    - 接続ファクトリーのプロパティ（*MQC*.XMSC_WMQ_OUTBOUND_SNI ）設定
    - 設定可能値
      - CHANNEL
      - HOSTNAME
      - * (アスタリスク)　→ ServerName=*でTLSのネゴシエーションを行う

.NETのXAモニターのTLS接続サポート

Multi.
V9.3.0/ V9.2.5

- .NETのXAモニター・アプリケーションがTLS接続をサポート
  - ◆ XAモニター・アプリケーション： WmqDotnetXAMonitor
    - 分散トランザクションをリカバリーするために使用
      - トランザクションが未確定であるキュー・マネージャーへの接続を確立し、設定したパラメーターに基づいてトランザクションをリカバリー
  - ◆ V9.2.5/V9.3.0以降、 キュー・マネージャーへのセキュア接続を使用可能
    - モニター・アプリケーションの起動引数またはアプリケーション構成ファイルにて、TLS接続のためのパラメータ設定が可能

MQIPT関連

- TLS 1.3サポート
  - ◆ 追加されたCipherSuite
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256

Multi.
V9.3.0 / V9.2.5

- TLS 1.2 までのCipherSuiteの追加・削除
  - ◆ 追加されたCipherSuite
    - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - ◆ 削除されたCipherSuite
    - SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
    - SSL_RSA_FIPS_WITH_DES_CBC_SHA

Multi.
V9.3.0 / V9.2.2

- FIPSモードの有効化方法の変更
  - ◆ 以下の指定を行う
    - com.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS
  - ◆ 以前の指定方法
    - com.ibm.jsse2.usefipsprovider=true

Multi.
V9.3.0 / V9.2.4 /
V9.2.0.5

Multi.
V9.3.0/ V9.2.5

■ 複数のキュー・マネージャー証明書のサポート

◆ SSLClientOutboundSNIプロパティの追加

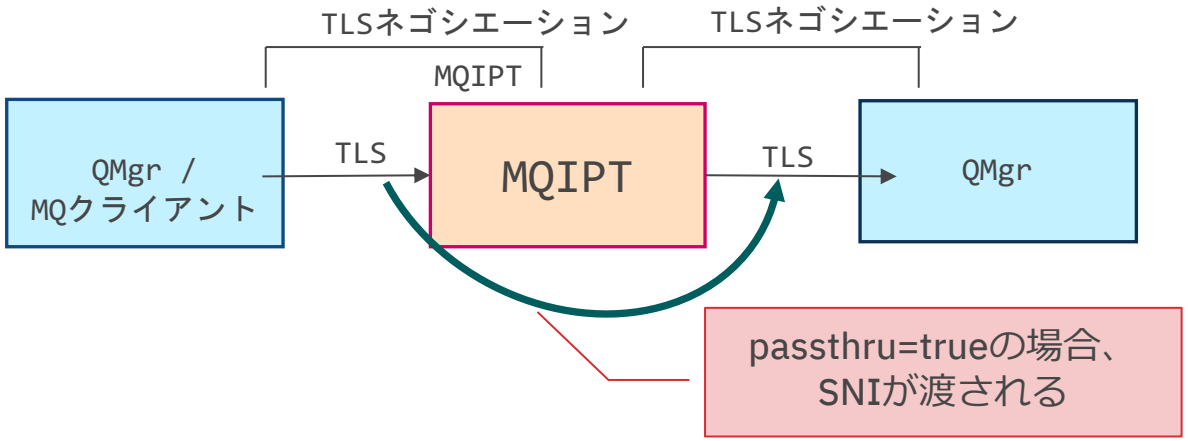
- MQIPT構成ファイルのルート・プロパティに追加
- キュー・マネージャーのデフォルト証明書を使用する　or チャネル毎の証明書を使用する
- SSLClient=trueの経路で有効

◆ 設定可能値

- hostname　：宛先ホスト名 (デフォルト値)
- channel　：接続先チャネル名
- passthru　：SSLServer=trueの場合、インバウンド接続のSNIがアウトバウンド接続に設定される
  TLS接続が無効の場合、ホスト名が設定される
- custom　：SSLClientCustomOutboundSNIで設定した値がSNIに設定される
- none　：SNI設定なし

◆ SSLClientCustomOutboundSNIプロパティ

- SSLClientOutboundSNI=custom設定時に
  参照されるプロパティ
- SNIを設定



ALW
V9.3.0/ V9.2.4

■ MQTT TLSチャネルの鍵リポジトリーパスワードの暗号化

◆ MQXRサービスの STARTARGオプションにて-sf または -spを指定して暗号化

- -sf : 鍵ファイルを指定
- -sp : 保護モードを指定

◆ MQXRサービスの定義例

```
SERVICE(SYSTEM.MQXR.SERVICE)           CONTROL(QMGR)
  SERVTYPE(SERVER)
  STARTCMD(+MQ_INSTALL_PATH+/mqxr/bin/runMQXRService.sh)
  STARTARG(-m +QMNAME+ -d "+MQ_Q_MGR_DATA_PATH+" -g "+MQ_DATA_PATH+" -sf "[DEFAULT]")
   :
```

- [DEFAULT]はMQが内部的に使用する鍵ファイル

◆ MQTTチャネルの定義・更新

- ALTER | DEFINE CHANNEL(channel_name) CHLTYPE(MQTT) SSLKEYP(パスワード)

→ パスワードが暗号化され、以下のプロパティファイルに保管される

- mqxr_win.properties （Windows）
- mqxr_unix.properties （AIX/Linux）

アプリケーション

Jakarta Messaging 3.0

- IBM MQ classes for Jakarta Messaging
  - ◆ MQ V9.3.0はJakarta Messagingのサポートを提供
    - 背景
      - JMSの仕様策定がOracleからJava Community Processに移管された
      - “javax”の使用権は引き続きOracleが保持
        - パッケージ名を”javax”から“jakarta”に変更
          - 例）javax.jms.Connection　→　jakarta.jms.Connection
      - Java EEのバージョン
        - Java EE 7：Oracle管理下、JMS 2.0が組み込まれている
        - Java EE 8：中間バージョン
        - Jakarta EE 9：”jakarta.”のPrefixが使用開始、Jakarta Messaging 3.0が組み込まれている

  - ◆ MQ V9.3では、Jakarta EE 9およびJakarta Messaging 3.0のサポートを開始
    - Java EE 7およびJMS 2.0、JMS 1.1のサポートも継続
    - 既存アプリケーションの継続使用は可能

Jakarta Messaging 3.0

共通
V9.3.0

- Java SE の提供内容
  - ◆ IBM MQ classes for JMS(JMS 2.0用)
  - ◆ IBM MQ classes for Jakarta Messaging
    - Jakarta Messaging 3.0 プロバイダーを提供
      - com.ibm.mq.jakarta.client.jar
- Jakarta EE 9の提供内容
  - ◆ Jakarta EE 9のアプリケーション・サーバーでMQベースのメッセージングをサポートするために、Jakarta EE 9互換のリソース・アダプター: wmq.jakarta.jmsra.rarを提供
  - ◆ Java EE 7互換のリソース・アダプター： wmq.jmsra.rarも引き続き提供
- JMS 2.0とJakarta Messaging 3.0の差異
  - ◆ Jakarta Messaging 3.0での新機能導入はなし

Jakarta Messaging 3.0

- MQ classes for JMS（JMSクラス） と MQ classes for Jakarta Messaging（Jakartaクラス） の差異
  - ◆ 概要
    - JMSクラスはJMS 2.0のサポートを提供
      - 主に既存アプリケーション向け
    - JakartaクラスはJakarta Messaging 3.0のサポートを提供
      - 新規アプリケーション向け
    - MQ V9.3.0において、JMSクラスとJakartaクラスの機能は同等、ネーミングのみ異なる
      - 今後の機能拡張はJakartaクラスにて行われる
    - 両者は相互接続が可能
      - JMSクラスがプロデューサー、Jakartaクラスがコンシューマーの構成は可能（逆も可能）
    - 同一アプリケーション内で両クラスの混在は不可
      - 1つのアプリケーションでJMSクラスとJakartaクラスを使用することはできない

Jakarta Messaging 3.0

◆ パッケージ名の変更

JMSクラスパッケージ名	Jakartaクラスパッケージ名
com.ibm.mq.jms [. *]	com.ibm.mq.jakarta.jms [. *]
com.ibm.jms	com.ibm.jakarta.jms
com.ibm.msg.client.jms. *	com.ibm.msg.client.jakarta.jms. *
com.ibm.msg.client.wmq. *	com.ibm.msg.client.jakarta.wmq. *

- プロパティ名の変更
  - JakartaクラスでMQ拡張機能を有効にするプロパティ名が変更
    - com.ibm.mq.jakarta.jms.SupportMQExtensions

（参考）Jakarta Messagingの全体像は以下を参照

- IBM MQ classes for Jakarta Messaging: an overview
  - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=messaging-mq-classes-jakarta-overview

Jakarta Messaging 3.0

- 管理ユーティリティ
  - crtmqenv / setmqenvコマンドに”-j”オプションの追加
    - -j 2.0：CLASSPATH 環境変数が変更され、 JMS 2.0 アプリケーションの実行に必要な JAR ファイルを組み込む　（デフォルト）
    - -j 3.0：CLASSPATH 環境変数が変更され、 Jakarta Messaging 3.0 アプリケーションの実行に必要な JAR ファイルを組み込む

```
[mqm@ISEP01 bin]$ . ./setmqenv -m QM930A -j 3.0
[mqm@ISEP01 bin]$ export
declare -x CLASSPATH="/opt/mqm9300/java/lib/com.ibm.mq.jakarta.client.jar"
```

  - dspmqverコマンドの戻り値でJakarta Messagingのサービス名を含めて結果を戻すように変更
    - dspmqver -p 4 （次ページにアウトプットイメージ）
  - JNDI管理ツールとしてJMS30Adminを提供
    - JMSAdminおよびMQ Explorerを使用してのJNDI管理は不可
- 開発・実行環境の設定
  - 導入ディレクトリー/java/bin以下に設定コマンドを提供
    - setjms30env　　32bit用
    - setjms30env64　　64bit用

共通
V9.3.0 /V9.2.4

toString() メソッドの動作変更

◆ toString()メソッドで接続情報を返す際に以下の情報を追加で返却(JSON形式)

- ObjectId
- ConnectionId
- ConnectionMode
- Host
- Port
- QueueManager
- ResolvedQueueManager

```
{"ConnectionId":"414D5143514D475232353031202020202020B4FDB362002E0040",
"ObjectId":"com.ibm.mq.MQQueueManager@49a0b795","Port":2501,
"Channel":"TO.QMGR2501.C2","ConnectionMode":"MQSeries Client",
"ResolvedQueueManager":"*","Host":"192.168.56.104","QueueManager":"*"}
```

◆ 動作変更対象のMQオブジェクト

- JMS・リソース・アダプター
  - MQConnection
  - MQSession
  - ConnectionFactory.createContext()で取得したオブジェクト
    - MQConnectionとMQSessionを内養蜂しているため
- BaseJava
  - MQQueueManager

Java関連

Multi.
V9.3.0 /V9.2.4

- MQクライアントにてJava 17をサポート
  - IBM MQ classes for Java（BaseJava)およびIBM MQ classes for JMS（JMS)にて Java 17のサポートを追加

Multi.
V9.3.0 /V9.2.1

- JMSクライアント・アプリケーションのデフォルト認証モードの変更
  - 接続認証機能（Connection Authentication）を使用して接続する際のデフォルト認証モードを変更
    - V9.3.0/ V9.2.1以降、MQCSP認証モードがデフォルト
      - V9.2.1以前は互換モードがデフォルト
      - BaseJavaではV9.2.1以前からMQCSPモードがデフォルト
  - 既存アプリケーションからの接続ができなくなる可能性があるため、以下の方法で認証モードを選択
以下、優先順位の高い順に記載
    - アプリケーションでの指定
      - JmsConstants.USER_AUTHENTICATION_MQCSP= false
    - Javaシステム・プロパティでの指定
      - java -Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=N *application_name*
    - 環境変数
      - com.ibm.mq.jmqi.useMQCSPauthentication=N
    - mqclient.iniのJMQIスタンザ
      - useMQCSPauthentication = NO

Java関連

Multi.
V9.3.0 /V9.2.5

- JavaアプリケーションのTLS接続時の注意点
  - ◆ OutbountSNI=CHANNEL使用時のチャネル名の制約が追加
    - チャネル名の最後の文字は大文字または数字であること
      - チャネル名の最後に小文字またはシンボルの使用は不可

Multi.
V9.3.0 /V9.2.2 /
V9.2.0.2

- Javaのチャネル出口プログラムでローカルアドレスを取得可能
  - ◆ `MQCD.getLocalAddress()`メソッドでローカル・アドレスを取得

.NETアプリケーション

Windows
V9.3.0

- MQ V9.3.0より.NET 6のサポートを開始

- .NET Framework およびXMS.NET Frameworkの前提をV4.7.2に変更
  - ◆ V9.2まではV4.6.2

- 管理コードの.NETクライアントアプリケーションのCCDT使用時の動作変更
  - ◆ V9.3.0より前のバージョンでは、グループ接続使用時の管理コード.NETクライアントと、Cクライアント/Javaクライアントの動作には違いがあった
    - 従来：QMGR名＝‘*’ の接続時にQMNAME=‘ ’（ブランク）以外のチャネルが使用される
    - V9.3.0以降： QMGR名＝‘*’ の接続時にQMNAME=‘ ’（ブランク）のチャネルがない場合には接続不可（MQRC_QMGR_NAME_ERROR）

    ＊非管理コードの.NETクライアントは従来からCクライアント/Javaクライアントと同じ動作

AMQP

ALW
V9.3.0

- AMQPアプリケーションでPtoP通信が可能
  - キューに対するメッセージ送信・受信が可能　[V9.2.1～]
  - メッセージのブラウズ機能の追加　[V9.2.2～]
- 動的キューが使用可能　[V9.2.3～]
  - 動的キューのためにAMQPチャネルに２つの属性を追加
    - TMPMODEL属性：一時キューの作成時に使用されるモデル・キューの名前
    - TMPQPRFX属性：一時キュー作成時のPrefix
- JAASログイン・モジュール・ファイルの移動　[V9.2.2～]
  - V9.3.0/V9.2.2より以下のロケーション
    - 導入Dir/amqp/samples/jaas/
  - V9.2.1まで：導入Dir/ amqp/samples/samples/
- Java Coreの出力抑止　[V9.2.5~/V9.2.0.5~]
  - 以下の設定でJava Core Dumpの出力制御が可能
    - com.ibm.mq.MQXR.GenerateJavaDump=false
  - プロパティファイルのロケーションが以下に変更
    - 導入Dir/qmgrs/qmgr_name/amqp/amqp_java.properties

ALW
V9.3.0

- JAASログイン・モジュール・ファイルの移動 [V9.2.2～]
  - ◆ V9.3.0/V9.2.2より以下のロケーション
    - 導入Dir/mqxr/samples/jaas/
  - ◆ V9.2.1まで
    - 導入Dir/mqxr/samples/samples/

- Java Coreの出力抑止 [V9.2.5~/V9.2.0.5~]
  - ◆ 以下の設定でJava Core Dumpの出力制御が可能
    - com.ibm.mq.MQXR.GenerateJavaDump=false
  - ◆ プロパティファイルのロケーションが以下に変更
    - 導入Dir/qmgrs/qmgr_name/mqxr/java.properties

Advanced関連

Advanced Message Security (AMS)

Multi.
V9.3.0 /V9.2.2

- パスワード保護機能の強化
  - ◆ Cクライアント用のAMS構成ファイル（keystore.conf）に保管するパスワードの暗号化が可能
    - V9.2まではJavaクライアント用の構成ファイルのみ保護が可能
      - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=securing-protecting-passwords-in-mq-component-configuration-files

- Bouncy Castle JARファイル名の変更
  - ◆ 再配布可能クライアント（BaseJava･JMS)に含まれるBouncy Caslte JAR ファイル名が以下の通り変更
    - bcpkix-jdk15to18.jar
    - bcprov-jdk15to18.jar
    - bcutil-jdk15to18.jar
  - ◆ V9.2以前は
    - bcpkix-jdk15on.jar
    - bcprov-jdk15on.jar

Managed File Transfer (MFT)

- 再配布可能MFTパッケージの拡張　　[V9.2.1~]
  - ◆ 再配布可能MFTパッケージにロガー機能を含む

- FTPエンドポイント毎のファイル転送制限　　[V9.2.1~]
  - ◆ プロトコル・ブリッジ経由で接続するFTPエンドポイントでのファイル転送制限が可能
    - ● 構成ファイルに新規属性が追加

- リソース・モニターの開始・終了方法の拡張　　[V9.2.2~]
  - ◆ fteStartMonitor / fteStopMonitorコマンドの追加
    - ● コマンド提供により、エージェントとは切り離してモニターの開始・終了が可能
    - ● これまではエージェントの起動・終了時にモニターが起動・終了
      - - モニター個別に任意のタイミングでの開始・終了が不可

- fteObfuscate コマンドによるCredential保護機能の強化　　[V9.2.4~]
  - ◆ V9.2.0よりユーザー・キーとより強力なアルゴリズムによる暗号化・復号化が可能
  - ◆ V9.3.0よりMD5ハッシュと最新のアルゴリズムによる暗号化・復号化が可能

Managed File Transfer (MFT)

共通
V9.3.0

- fteRASコマンドの拡張　　[V9.2.4~]
  - ◆ 進捗状況がコンソールに表示
    - 各ステップの開始・終了時刻、圧縮関連情報、など
      - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=reference-fteras-collect-mft-troubleshooting-information

- 転送ログの拡張
  - ◆ 転送ログに転送成功/転送不成功に加えて詳細情報を出力　　[V9.2.4～]
  - ◆ fteSetAgentLogLevel コマンドにlogTransferオプションの追加　　[V9.2.4～]
  - ◆ 新規ログファイルtransferlog0.jsonが出力されるように変更　　[V9.2.5～]
    - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=reference-output-produced-by-logtransfer-function

- MFTコマンドにてMQCSP認証モードをデフォルトに変更　　[V9.3.0~]
  - ◆ MFTコマンド実行時に調整・コマンド・エージェントの各キュー・マネージャーに接続する際に、MQCSP認証モードで接続するよう変更された
    - 下位のキュー・マネージャーに接続するためのオプションも追加

Managed File Transfer (MFT)

共通
V9.3.0

- REST APIによるManagedCall [V9.3.0~]
  - ◆ Managed Callとは、MFTエージェントを使用してスクリプトやJCL等をCallし実行すること
  - ◆ Managed CallにてREST API V3のVerb（POST/GET)を使用可能

- 転送ログの変更 [V9.2.4~]
  - ◆ リソース・モニター・ログ
    - agent.propertiesのrecourceMonitorLogFilesのデフォルト値が5
      - V9.2.3まではデフォルト10
  - ◆ プロトコル・ブリッジ・エージェント・ログ
    - agent.propertiesのagentLogFilesのデフォルト値が5
      - V9.2.3までデフォルト10

- fteStopAgentコマンド発行後のステータス追加 [V9.3.0~]
  - ◆ fteStopAgentコマンド発行後、”STOPPING”のステータスが表示される
    - コマンド発行後、処理中の転送が終了するまでの間のステータス
    - V9.2まではコマンド発行後すぐに“STOPPED”ステータスとなった
      - 実際にはしかかり中の転送が実行されていた

Managed File Transfer (MFT)

- File to Messageの転送時のデリミターサイズエラー動作変更　[V9.2.2~/V9.2.0.2~]
  - ◆ デリミターのサイズエラーの場合、ブランク・メッセージが1件送信される
- エージェント・プロパティのstandbyPollIntervalの拡張　　[V9.2.4~/V9.2.0.5~]
  - ◆ 高可用性構成のプロパティstandbyPollIntervalで、エージェント・キュー・マネージャーへの再接続のインターバルを設定
- モニター・リクエストのXMLスキーマ変更　　[V9.2.5~/V9.2.0.5~]
  - ◆ Monitor.xsdスキーマのdirectory エレメントの maxOccurs 属性は 1に設定
    - これまではunbounded設定

Aspera gateway

共通
V9.3.0

- サポートバージョンの変更
  - IBM Aspera fasp.io. Gatewayのサポートバージョンが**V1.2.0**に変更(V9.2.3～)
    - これに伴いディレクトリの変更などが行われた
      - https://www.ibm.com/docs/en/ibm-mq/9.2?topic=configuring-defining-aspera-gateway-connection-linux-windows
      - https://www.ibm.com/docs/en/faspio-gateway/1.2?topic=release-notes-aspera-faspio-gateway-12

メッセージの追加・変更・削除

メッセージの追加・変更・削除

共通
V9.3.0

- V9.3.0にて、追加・変更・削除されたメッセージ
  - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=930-new-changed-removed-messages-in-mq
- V9.2.5以降で、追加・変更・削除されたメッセージ
  - https://www.ibm.com/docs/en/ibm-mq/9.3?topic=930-new-changed-removed-messages-since-mq-925
- V9.2.xで追加・変更・削除されたメッセージは、各CDの変更点を確認すること
  - What‘s new and changed in IBM MQ 9.2.x Continuous Delivery ページ
    - https://www.ibm.com/docs/en/ibm-mq/9.2?topic=am-whats-new-changed-in-mq-92x-continuous-delivery

Deprecated / Stabilized / Removed

Deprecated / Stabilized / Removed

共通
V9.3.0

- Deprecated
  - AMSで使用できるCipher（一部）
  - 32bitクライアントライブラリ
  - SSLv3、TLS 1.0(V9.2～)
  - MFTでfteObfuscate コマンドの-credentialsFile引数
  - MFTにて、FTEで始まる環境変数（V9.2.0～）
- Stabilized
  - amqmdnet.dll library (V9.2.0～)
  - IBM.XMS.* libraries (V9.2.0～)
- Removed
  - Dashboard Webコンソール
  - XMS .NET Multicast messaging
  - MFTの移行コマンド（fteMigrateAgent, fteMigrateConfigurationOptions, fteMigrateLogger）
    - V7.0以前のMFT環境を移行するコマンド、V9.2.1で提供終了

詳細は以下のKnowledge Centerの記述を確認のこと

- MQ V9.3: https://www.ibm.com/docs/en/ibm-mq/9.3?topic=930-deprecated-stabilized-removed-features-in-mq
- MQ V9.2.x: https://www.ibm.com/docs/en/ibm-mq/9.2?topic=am-whats-new-changed-in-mq-92x-continuous-delivery
  - 各CDの新機能・変更点から確認のこと