Collecte et Exportation des logs & events MQ en format json

Luc-Michel DEMEY - Demey Consulting
lmd@demey-consulting.fr

Version 1.0.4 - Avril 2022

Contexte

- Société de gestion d'actifs (valeurs mobilières & immobilières)
- Filiale d'un groupe européen de bancassurance
- Utilisation du réseau Swift via IBM MQ
  - donc architecture type A4 (ex "B")
- Queue Manager en mode QMMI, hébergé sur des VM Windows, MQ version 9.2.x
- Mise en place du Swift CSP (Customer Security Programme)

Principes du SWIFT CSP

- Réduire la surface d'attaque et les vulnérabilités
- Gérer les identités et séparer les privilèges
- Segmenter ou isoler les réseaux
- Chiffrer les flux sensibles
- Détecter les évènements de sécurité et les activités anormales sur les systèmes

Framework de contrôle CSP :

- Comprend 22 contrôles de sécurité obligatoires et 9 contrôles facultatifs
- Evaluation indépendante (externe) à partir de 2022

Détecter les évènements de sécurité

- Logs techniques de tous les composants de la zone sécurisée Swift.
- Accès (succès et échecs de connexion, déconnection, changement de configuration, élévation de privilèges, …)
- Logs des Firewall
- Logs conservés 31 jours et exportés à l'extérieur du serveur
- Evènements de sécurité à mapper vers l'environnement MQ

Objectif du projet

- Identifier les évènements MQ pertinents pour le CSP
- Collecter les données correspondantes
- Exporter ces données vers l'extérieur sous une forme utilisable
- Figures imposées :
  - Serveurs MQ Windows
  - Configuration QMMI
  - Stockage des évènements dans Azure Sentinel
- A définir :
  - Mode et format de collecte
  - Mode d'envoi à Sentinel

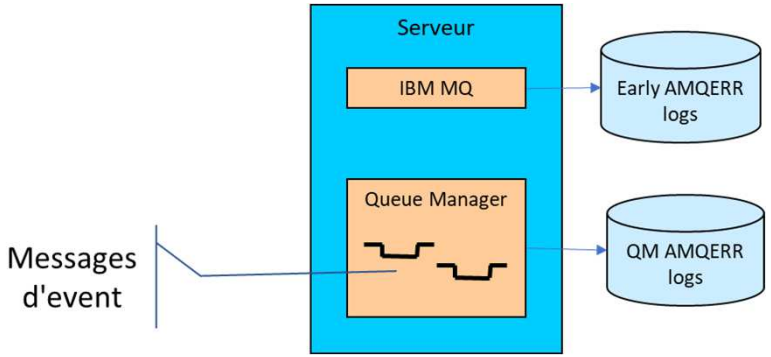
Note : pas d'exploitation des logs imposée par CSP côté Sentinel !

Evènements MQ

- Création / démarrage / arrêt / suppression des QM
- Changements de configuration MQ
- Violations de sécurité MQ
- Erreurs lors de l'accès aux files MQ locales (file pleine, absente, ...)
- Changement d'état et erreurs liées aux canaux
- Erreurs liées à SSL/TLS (certificats invalides, expirés, ...)

Collecter

- Observateur d'événements Windows :
  - Sous-ensemble uniquement, incomplet
- Eléments pertinents :
  - les AMQERR logs (early & QM)
    - Logs texte, disponibles également en format json
  - les events MQ
    - Sous forme de messages dans des files MQ techniques
    - Outils pour exporter ces messages vers des fichiers plats en format texte ou json.



Collecte des AMQERR

- Liés à l'installation MQ → mqs.ini (Early AMQERR)
- Liés à un Queue Manager → qm.ini (QM AMQERR)
- Rotation des fichiers
  - le fichier AMQERR01.LOG est toujours le plus récent
  - à prendre en compte pour le mécanisme d'export

Paramétrage pour les Early AMQERR

- Dans le mqs.ini, ajout du bloc :

```
DiagnosticSystemMessages:
   Service=File
   Name=JSONLogs
   Format=json
   FilePrefix=AMQERR
```

- Avec cet ajout, les fichiers .json seront créés dans le même répertoire que les fichiers .LOG.
- Rotation : identique aux AMQERRxx.LOG.
- Prise en compte : immédiate

Paramétrage pour les QM AMQERR

- Dans le qm.ini, ajout du bloc :

```
DiagnosticMessages:
          Service = File
          Name = JSONLogs
          FilePath = E:\mq\qmgrs\<nom_qm>\json
          FilePrefix = AMQERR
          Format = json
```

- FilePath: permet de spécifier un chemin différent du défaut
- La chaine <nom_qm> est à remplacer par le nom du Queue Manager
- Rotation : identique aux AMQERRxx.LOG.
- Prise en compte : redémarrage du QM

Collecte des events MQ - Principe

- Stockés sous forme de messages MQ
- Activation via des paramètres du QM
- Utilitaire amqsevt pour les lire / convertir les events

Activation des events MQ

- Par défaut, quasiment aucun event n'est activé.
- Activation via MQSC
- Exemple pour un QM avec des logs linéaires :

```
ALTER QMGR +
   AUTHOREV (ENABLED) +
   INHIBTEV (ENABLED) +
   LOCALEV (ENABLED) +
   REMOTEEV (ENABLED) +
   STRSTPEV (ENABLED) +
   CHLEV (EXCEPTION) +
   SSLEV (ENABLED) +
   CHADEV(ENABLED) +
   PERFMEV (ENABLED) +
   CONFIGEV (ENABLED) +
   CMDEV (NODISPLAY) +
   LOGGEREV(ENABLED)
```

Lecture des events MQ

- IBM fournit un utilitaire (**amqsevt**) qui permet de lire les messages d'event dans ces files, et de les restituer sous forme de fichiers.
- L'option "`json_compact` » permet d'obtenir des fichiers où chaque évènement est restitué sous la forme d'une seule ligne au format json. Cette option est disponible à partir de MQ version 9.2.3.

```
Usage: amqsevt [-m Qmgr] [-r d|r|m] [-b] [-c] [-d] [-o format]
         [-u User ID] [-w wait] {-t Topic} {-q Queue}
  -m <Queue Manager Name>
  -t <Topic> Can have multiple entries
  -q <Queue> Can have multiple entries
  -b Browse messages
  -c Connect as client
  -d Print definitions without formatting
  -o <Output format>
     json
     json_compact
     json_array
     text (default)
  -r <Reconnect Type>
     d Reconnect Disabled
     r Reconnect
     m Reconnect Queue Manager
  -u User ID
  -w <Wait time in seconds>
```

Passage des events en mode PubSub

- Events MQ :
  - Par défaut déposés dans des files locales (SYSTEM.ADMIN.xxx.EVENT)
  - Multiconsommateurs ?
    - MQ Explorer
    - Outils de supervision
    - …
- Passage en mode PubSub :
  - Remplacement des files locales SYSTEM.ADMIN.xxx.EVENT par des files alias de même nom
  - Files alias qui pointent vers un topic, par exemple SYSTEM.ADMIN.EVENT
  - Création de deux files locales spécifiques, et abonnement administratif de ces deux files au topic SYSTEM.ADMIN.EVENT.

Caractéristiques des files

- La file SYSTEM.ADMIN.SUBSCRIBED.EVENT est le nom par défaut connu du plugin MS0P de MQ Explorer pour lire les messages d'event (ce qui permettra à MQ Explorer de continuer à exploiter les events)
- La file SYSTEM.ADMIN.AMQSEVT.EVENT contiendra les messages d'event à convertir en fichier json
- La persistance des messages est forcée à YES, afin que le contenu des files puisse survivre à un redémarrage du Queue Manager
- Le paramètre CAPEXIRY (= rétention) est réglé à 10 jours (8640000 x 1/10 de secondes) pour les messages à consommer par MQ Explorer, et à 10 jours également pour la file utilisée pour générer les fichiers json.

Configuration du mode PubSub (1/4)

- Création du topic SYSTEM.ADMIN.EVENT :

```
DEFINE TOPIC(SYSTEM.ADMIN.EVENT) +
    TOPICSTR('SYSTEM/ADMIN/EVENT') +
    REPLACE
```

- Exemple pour la file SYSTEM.ADMIN.CHANNEL.EVENT
  - À faire pour toutes les files d'event)

```
DELETE QLOCAL(SYSTEM.ADMIN.CHANNEL.EVENT) PURGE
DEFINE QALIAS(SYSTEM.ADMIN.CHANNEL.EVENT)     +
    TARGET(SYSTEM.ADMIN.EVENT) +
    TARGTYPE(TOPIC) +
    DEFPSIST(YES) REPLACE
```

Configuration du mode PubSub (2/4)

```
* Creation de la file locale pour lecture par MQ Explorer / MS0P
DEFINE QLOCAL(SYSTEM.ADMIN.SUBSCRIBED.EVENT) +
    CUSTOM('CAPEXPRY(8640000)') +
    MAXDEPTH(15000) +
    DEFPSIST(YES) +
    REPLACE +
    DESCR('Events MQ pour MQExplorer - MS0P')

* Creation de la file locale pour consommation par amqsevt
DEFINE QLOCAL(SYSTEM.ADMIN.AMQSEVT.EVENT) +
    CUSTOM('CAPEXPRY(864000)') +
    MAXDEPTH(15000) +
    DEFPSIST(YES) +
    REPLACE +
    DESCR('Events consommation par amqsevt')
```

Configuration du mode PubSub (3/4)

```
* Souscription administrative pour SYSTEM.ADMIN.SUBSCRIBED.EVENT (MS0P)
DEFINE SUB(SYSTEM.ADMIN.EVENT) +
    TOPICOBJ(SYSTEM.ADMIN.EVENT) +
    DEST(SYSTEM.ADMIN.SUBSCRIBED.EVENT) +
    REPLACE

* Souscription administrative pour SYSTEM.ADMIN.AMQSEVT.EVENT
DEFINE SUB(SYSTEM.ADMIN.AMQSEVT.EVENT) +
    TOPICOBJ(SYSTEM.ADMIN.EVENT) +
    DEST(SYSTEM.ADMIN.AMQSEVT.EVENT) +
    REPLACE
```

Configuration du mode PubSub (4/4)

- Résultat :
  - File locale SYSTEM.ADMIN.AMQSEVT.EVENT
    - Contenant tous les types d'events activés
    - Consommée par le script extract_events.bat
  - File locale SYSTEM.ADMIN.SUBSCRIBED.EVENT
    - Contenant tous les types d'events activés
    - Consommée par le plugin MS0P de MQ Explorer
  - Si une nouvelle application souhaite consommer les events MQ , il suffit de lui créer une file et d'abonner cette file au topic SYSTEM.ADMIN.EVENT

Génération des fichiers d'event json

- Script extract_events.bat lancé par trigger MQ
- Commande :

```
amqsevt -m %QM% -q %EventQ% -w %WaitTime% -o json_compact > %PathJson%\%EventJson%
```

- EventJson : nom du fichier de sortie
  - Format : nom_QM_amqsevt_AAAA-MM-JJ_HH-MM-SS.json
- WaitTime : nombre de secondes avant arrêt de amqsevt une fois tous les events traités
  - arbitrairement fixé à 60 (secondes).

```
@echo off
Rem ****************************************
Rem * Extraction des events MQ - Fichier extract_events.bat
Rem * Sortie %PathJson% sur un path local car UNC ko avec Sentinel
Rem * Gestion du nom de fichier si heure < 10h00
Rem * Version pour MQ 925 (924 mini)
Rem * LM Demey - 21/03/2022
Rem ****************************************
echo *** Extraction des events MQ en format json ****
set RunDate=%date:~-4,4%-%date:~-7,2%-%date:~-10,2%
Rem * gestion si heure < 10h00
set heure=%time:~0,2%
if "%heure:~0,1%" == " " set heure=0%heure:~1,1%
set RunTime=%heure%-%time:~3,2%-%time:~6,2%
set QM=%2
set EventQ=SYSTEM.ADMIN.AMQSEVT.EVENT
set PathJson=E:\mq\qmgrs\%QM%\events
set EventJson=%QM%_amqsevt_%RunDate%_%RunTime%.json
set WaitTime=60
echo QM : %QM%
echo Path json: %PathJson%
echo EventQ : %EventQ%
echo RunDate=%RunDate%
echo RunTime=%RunTime%
echo EventJson=%EventJson%
echo WaitTime=%WaitTime%
echo Extraction des events en cours dans %PathJson%\%EventJson% ...
amqsevt -m %QM% -q %EventQ% -w %WaitTime% -o json_compact > %PathJson%\%EventJson%
echo *** Fin de l'extraction ***
exit
```

```
* Extraction des events en json
* Fichier extract_events.mqsc
* LM Demey 21/03/2022

DEFINE QLOCAL(SYSTEM.ADMIN.AMQSEVT.INIT) +
  REPLACE +
  DESCR('InitQ pour extract events')

ALTER QLOCAL(SYSTEM.ADMIN.AMQSEVT.EVENT) +
  TRIGGER +
  PROCESS(AMQSEVT) +
  INITQ(SYSTEM.ADMIN.AMQSEVT.INIT)

DEFINE PROCESS(AMQSEVT) +
  APPLICID('\\PartageMQ\scripts\extract_events.bat') +
  ENVRDATA(QMP01) +
  DESCR('Process pour extract events') +
  REPLACE

DEFINE SERVICE('TRIGMON_E') +
   CONTROL(QMGR) +
   SERVTYPE(SERVER) +
   STARTCMD('+MQ_INSTALL_PATH+\bin\runmqtrm.exe') +
   STARTARG('-m +QMNAME+ -q SYSTEM.ADMIN.AMQSEVT.INIT') +
   STDOUT('E:\mq\qmgrs\+QMNAME+\events\runmqtrm.stdout') +
   STDERR('E:\mq\qmgrs\+QMNAME+\events\runmqtrm.stderr') +
   DESCR('Trigger Monitor pour AMQSEVT') +
   REPLACE

CLEAR QLOCAL(SYSTEM.ADMIN.AMQSEVT.EVENT)
START SERVICE('TRIGMON_E') IGNSTATE(YES)
*
```

Résultat - Logs AMQERR "installation"

Format texte

```
3/11/2022 11:41:08 - Process(2144.1) User(Admin-Demey-T1OP) Program(setmqinst.exe)
                     Host(MQUAT01) Installation(Installation1)
                     VRMF(9.2.5.0)
                     Time(2022-03-11T10:41:08.077Z)
                     CommentInsert1(advanced)
                     CommentInsert2(E:\mq)
AMQ5768I: Licensed entitlement 'advanced' unset for installation at 'E:\mq'.
EXPLANATION:
The licensed entitlement 'advanced' has been unset for installation at 'E:\mq'.
ACTION: None.
----- amqiset0.c : 1876 --------------------------------------------------------
3/11/2022 11:41:31 - Process(7872.1) User(Admin-Demey-T1OP) Program(setmqinst.exe)
                     Host(MQUAT01) Installation(Installation1)
                     VRMF(9.2.5.0)
                     Time(2022-03-11T10:41:31.711Z)
                     CommentInsert1(Installation1)
                     CommentInsert2(E:\mq)
AMQ8576I: 'Installation1' (E:\mq) set as the primary installation. You must
restart the operating system to complete the update.
EXPLANATION:
All tasks required to set installation 'Installation1' as the primary
installation have been completed. If the installation was not already set as
the primary installation then the Installation Configuration has also been
updated to identify installation 'Installation1' as the primary installation.
```

Format json


```
{"ibm_messageId":"AMQ5768I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":"advanced","ibm_commentInsert2":"E:\\mq","ibm_datetime":"2022-03-11T10:41:08.077Z","type":"mq_log","host":"MQUAT01","loglevel":"INFO","module":"amqiset0.c:1876","ibm_sequence":"1646995268077685_1585052875003","ibm_processId":"2144","ibm_threadId":"1","ibm_version":"9.2.5.0","ibm_processName":"setmqinst.exe","ibm_userName":"Admin-Demey-T1OP","ibm_installationName":"Installation1","ibm_installationDir":"E:\\mq","message":"AMQ5768I: Licensed entitlement 'advanced' unset for installation at 'E:\\mq'."}

{"ibm_messageId":"AMQ8576I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":"Installation1","ibm_commentInsert2":"E:\\mq","ibm_datetime":"2022-03-11T10:41:31.711Z","type":"mq_log","host":"MQUAT01","loglevel":"INFO","module":"amqiprm0.c:395","ibm_sequence":"1646995291711974_1585287207055","ibm_processId":"7872","ibm_threadId":"1","ibm_version":"9.2.5.0","ibm_processName":"setmqinst.exe","ibm_userName":"Admin-Demey-T1OP","ibm_installationName":"Installation1","ibm_installationDir":"E:\\mq","message":"AMQ8576I: 'Installation1' (E:\\mq) set as the primary installation. You must restart the operating system to complete the update."}
```

Résultat - Events format json

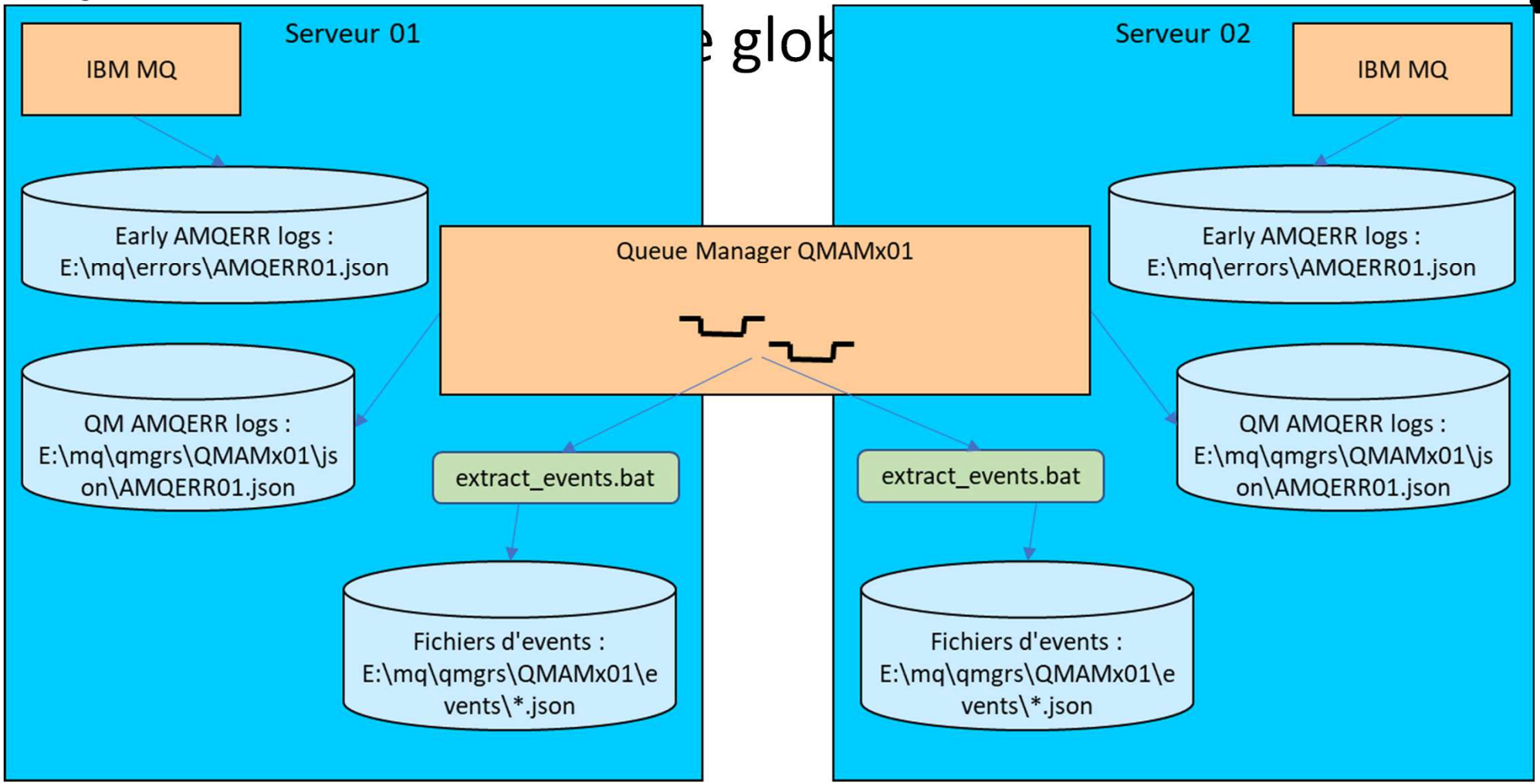

```
1  { "eventSource" : { "objectName": "SYSTEM.ADMIN.AMQSEVT.EVENT",  "objectType" : "Queue",  "queueMgr" : "QMR01"}, "eventType" : {  "name" : "Config
   Event",  "value" : 43  }, "eventReason" : {  "name" : "Config Change Object",  "value" : 2368  }, "eventCreation" : {  "timeStamp"  : "2022-03-11T11:05:20Z",  "epoch"
   : 1646996720  }, "objectState" : "Before Change", "correlationID" : "414D51204C46414D5230312020202035D41D6223F1C23C", "eventData" : {  "eventUserId" : "adm_full",
   "eventSecurityId" : "1D0101050000000000051500000030006B7BF45F5A64772C315D2461000000000000000000000000",  "eventOrigin" : "Msg",  "eventQueueMgr" : "QMR01",  "eventAccountingToken" :
   "160105150000030006B7BF45F5A64772C315D24610000000000000000000000B",  "eventApplIdentity" : "",  "eventApplType" : "Java",  "eventApplName" : "MQ Explorer 9.2.4",  "eventApplOrigin" :
    "",  "objectType" : "Queue",  "queueName" : "TEST3",  "queueDesc" : "",  "processName" : "",  "backoutReqQueueName" : "",  "initiationQueueName" : "",  "triggerData" : "",
   "clusChlName" : "",  "custom" : "",  "clusterName" : "",  "clusterNamelist" : "",  "streamQueueName" : "",  "creationDate" : "2019-12-13",  "creationTime" : "09.08.29",
   "alterationDate" : "2019-12-13",  "alterationTime" : "09.08.29",  "inhibitGet" : "Get Allowed",  "inhibitPut" : "Put Allowed",  "defPriority" : 0,  "defPersistence" : "Not
   Persistent",  "maxQueueDepth" : 5000,  "maxMsgLength" : 4194304,  "backoutThreshold" : 0,  "shareability" : "Shareable",  "defInputOpenOption" : "Input Shared",  "hardenGetBackout"
    : "Backout Hardened",  "msgDeliverySequence" : "Priority",  "retentionInterval" : 999999999,  "usage" : "Normal",  "triggerControl" : "Off",  "triggerType" : "First",
   "triggerDepth" : 1,  "triggerMsgPriority" : 0,  "queueDepthHighLimit" : 80,  "queueDepthLowLimit" : 20,  "queueDepthMaxEvent" : "Enabled",  "queueDepthHighEvent" : "Disabled",
   "queueDepthLowEvent" : "Disabled",  "queueServiceInterval" : 999999999,  "queueServiceIntervalEvent" : "Disabled",  "distLists" : "Not Supported",  "npmClass" : "Class Normal",
   "statisticsQueue" : "Queue Mgr",  "accountingQueue" : "Queue Mgr",  "monitoringQueue" : "Queue Mgr",  "scope" : "Queue Mgr",  "defBind" : "Bind On Open",  "clwlQueueRank" : 0,
   "clwlQueuePriority" : 0,  "clwlUseq" : "Useq As Queue Mgr",  "defPutResponseType" : "Sync Response",  "defReadAhead" : "No",  "propertyControl" : "Compatibility",
   "mediaImageRecoverQueue" : "As Queue Mgr",  "maxQueueFileSize" : "Default",  "streamQueueQos" : 0,  "definitionType" : "Predefined",  "queueType" : "Local" } }
2  { "eventSource" : { "objectName": "SYSTEM.ADMIN.AMQSEVT.EVENT",  "objectType" : "Queue",  "queueMgr" : "QMR01"}, "eventType" : {  "name" : "Config
   Event",  "value" : 43  }, "eventReason" : {  "name" : "Config Change Object",  "value" : 2368  }, "eventCreation" : {  "timeStamp"  : "2022-03-11T11:05:20Z",  "epoch"
   : 1646996720  }, "objectState" : "After Change", "correlationID" : "414D51204C46414D5230312020202035D41D6223F1C23C", "eventData" : {  "eventUserId" : "adm_full",
   "eventSecurityId" : "1D0101050000000000051500000030006B7BF45F5A64772C315D2461000000000000000000000000",  "eventOrigin" : "Msg",  "eventQueueMgr" : "QMR01",  "eventAccountingToken" :
   "160105150000030006B7BF45F5A64772C315D24610000000000000000000000B",  "eventApplIdentity" : "",  "eventApplType" : "Java",  "eventApplName" : "MQ Explorer 9.2.4",  "eventApplOrigin" :
    "",  "objectType" : "Queue",  "queueName" : "TEST3",  "queueDesc" : "",  "processName" : "",  "backoutReqQueueName" : "",  "initiationQueueName" : "",  "triggerData" : "",
   "clusChlName" : "",  "custom" : "",  "clusterName" : "",  "clusterNamelist" : "",  "streamQueueName" : "",  "creationDate" : "2019-12-13",  "creationTime" : "09.08.29",
   "alterationDate" : "2022-03-11",  "alterationTime" : "12.05.20",  "inhibitGet" : "Get Allowed",  "inhibitPut" : "Put Allowed",  "defPriority" : 0,  "defPersistence" : "Not
   Persistent",  "maxQueueDepth" : 5000,  "maxMsgLength" : 4194304,  "backoutThreshold" : 0,  "shareability" : "Shareable",  "defInputOpenOption" : "Input Shared",  "hardenGetBackout"
    : "Backout Hardened",  "msgDeliverySequence" : "Priority",  "retentionInterval" : 999999999,  "usage" : "Normal",  "triggerControl" : "Off",  "triggerType" : "First",
   "triggerDepth" : 1,  "triggerMsgPriority" : 0,  "queueDepthHighLimit" : 80,  "queueDepthLowLimit" : 20,  "queueDepthMaxEvent" : "Enabled",  "queueDepthHighEvent" : "Disabled",
   "queueDepthLowEvent" : "Disabled",  "queueServiceInterval" : 999999999,  "queueServiceIntervalEvent" : "Disabled",  "distLists" : "Not Supported",  "npmClass" : "Class Normal",
   "statisticsQueue" : "Queue Mgr",  "accountingQueue" : "Queue Mgr",  "monitoringQueue" : "Queue Mgr",  "scope" : "Queue Mgr",  "defBind" : "Bind On Open",  "clwlQueueRank" : 0,
   "clwlQueuePriority" : 0,  "clwlUseq" : "Useq As Queue Mgr",  "defPutResponseType" : "Sync Response",  "defReadAhead" : "No",  "propertyControl" : "Compatibility",
   "mediaImageRecoverQueue" : "As Queue Mgr",  "maxQueueFileSize" : "Default",  "streamQueueQos" : 0,  "definitionType" : "Predefined",  "queueType" : "Local" } }
3  { "eventSource" : { "objectName": "SYSTEM.ADMIN.AMQSEVT.EVENT",  "objectType" : "Queue",  "queueMgr" : "QMR01"}, "eventType" : {  "name" : "Command
   Event",  "value" : 99  }, "eventReason" : {  "name" : "Command PCF",  "value" : 2413  }, "eventCreation" : {  "timeStamp"  : "2022-03-11T11:05:20Z",  "epoch"  :
   1646996720  }, "correlationID" : "414D51204C46414D5230312020202035D41D6223F1C23C", "eventData" : { "commandContext" : {  "eventUserId" : "adm_full",  "eventSecurityId" :
   "1D0101050000000000051500000030006B7BF45F5A64772C315D2461000000000000000000000000",  "eventOrigin" : "Msg",  "eventQueueMgr" : "QMR01",  "eventAccountingToken" :
   "160105150000030006B7BF45F5A64772C315D24610000000000000000000000B",  "eventApplIdentity" : "",  "eventApplType" : "Java",  "eventApplName" : "MQ Explorer 9.2.4",  "eventApplOrigin" :
    "",  "command" : "Change Queue" }, "commandData" : {  "queueName" : "TEST3",  "queueType" : "Local",  "queueDesc" : "" }  } }
4
```

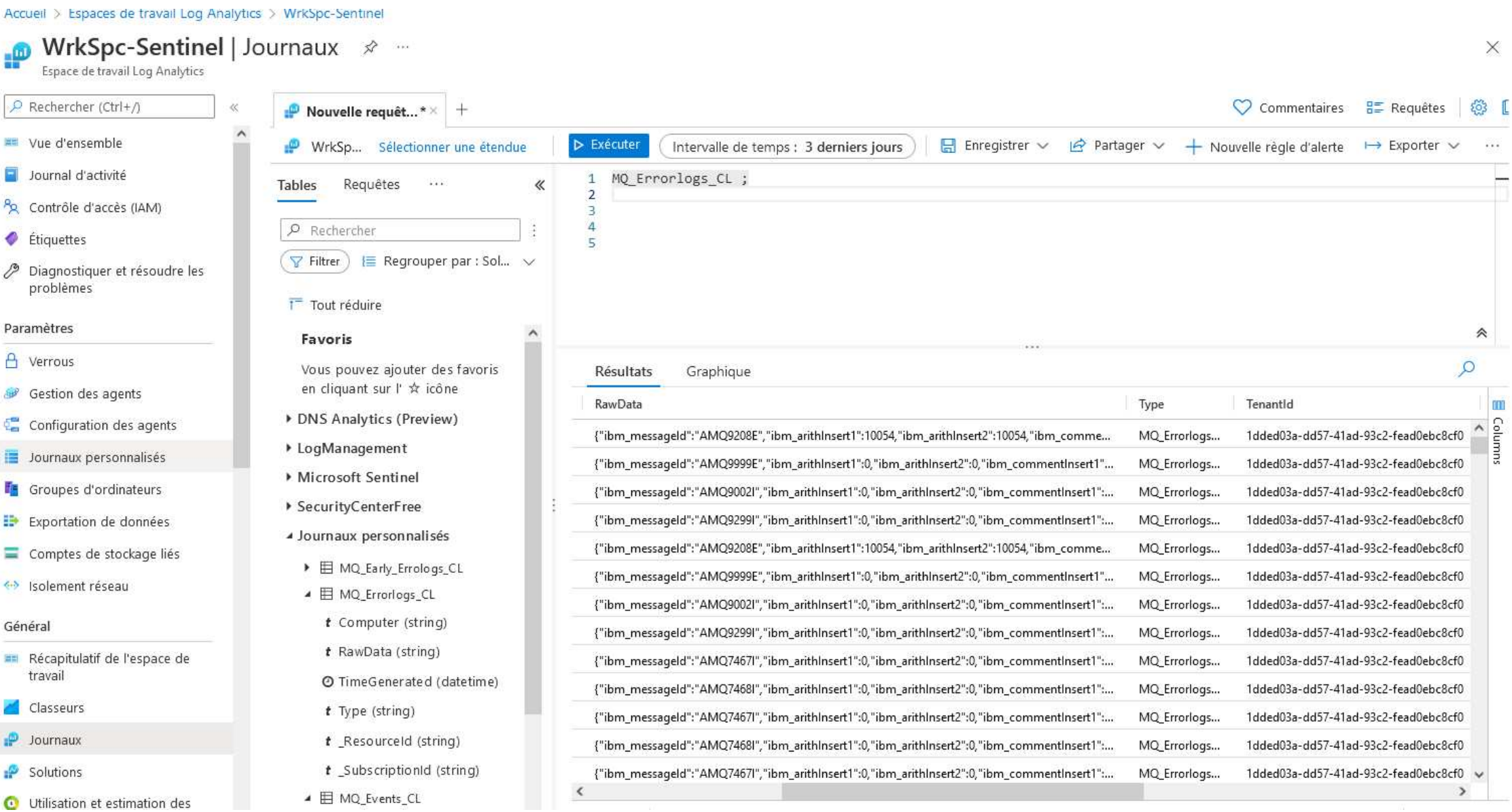
Impact du QMMI

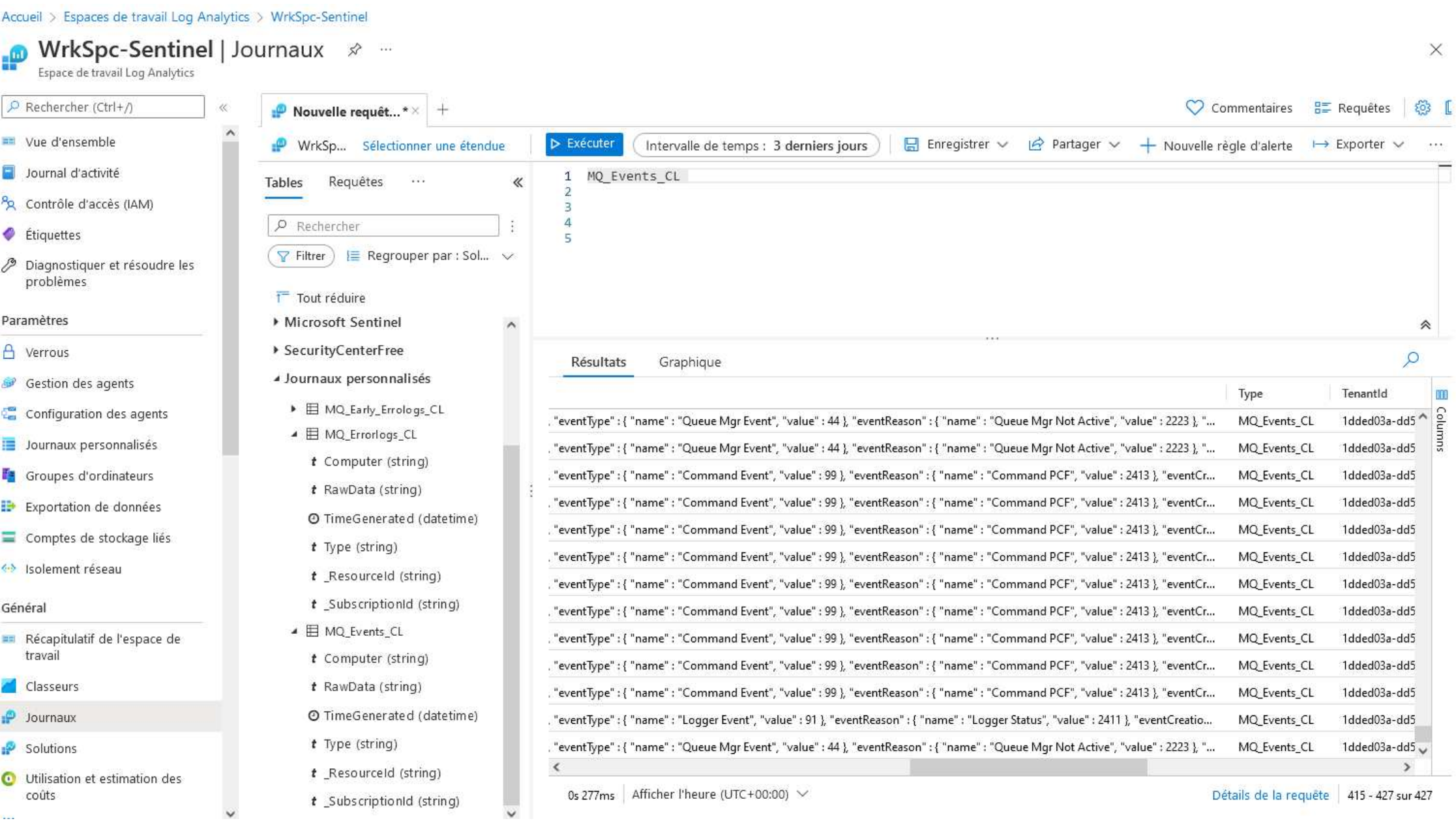
- 2 x installations MQ
- 1 QM avec données sur disque partagé
- 2 solutions :
  - Logs json sur partage disque
  - Logs json sur disque local
- Réponse : dépend du mode de collecte
  - agent démarré par l'OS
  - agent démarré par le QM

Collecte & envoi des fichiers json

- Utilisation de l'agent OMS Windows (Operations Management Suite)
  - Un agent tourne en permanence sur chaque serveur
- Fichiers remontés sur l'application Azure Sentinel
- Donc :
  - Fichiers json générés sur le disque local de chaque serveur
    - Evite les remontées en double

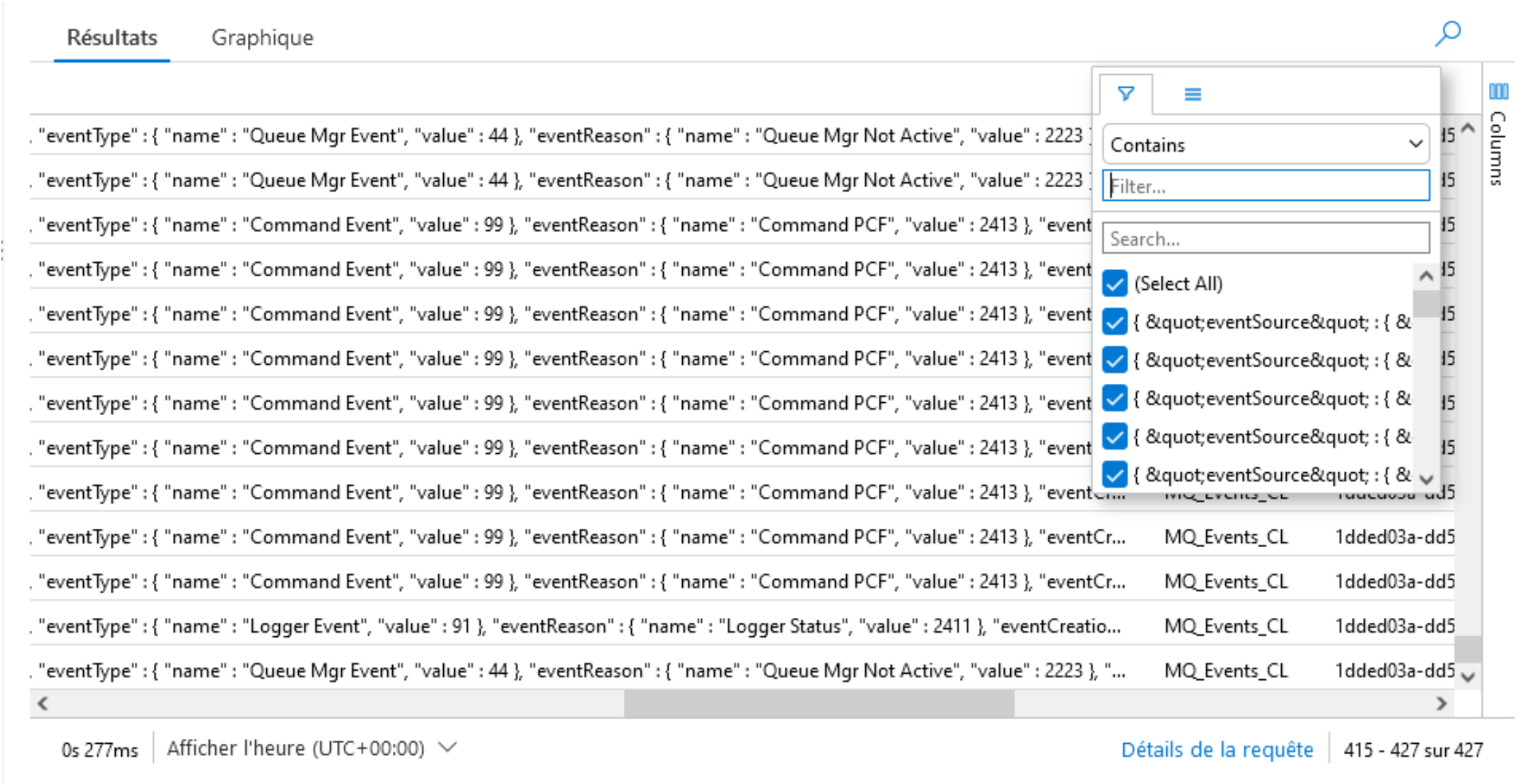



Accueil > Espaces de travail Log Analytics > WrkSpc-Sentinel
WrkSpc-Sentinel | Journaux
Espace de travail Log Analytics
Rechercher (Ctrl+/)
Vue d'ensemble
Journal d'activité
Contrôle d'accès (IAM)
Étiquettes
Diagnostiquer et résoudre les problèmes
Paramètres
Verrous
Gestion des agents
Configuration des agents
Journaux personnalisés
Groupes d'ordinateurs
Exportation de données
Comptes de stockage liés
Isolement réseau
Général
Récapitulatif de l'espace de travail
Classeurs
Journaux
Solutions
Utilisation et estimation des
Nouvelle requêt... *
Commentaires
Requêtes
WrkSp...
Sélectionner une étendue
Exécuter
Intervalle de temps : 3 derniers jours
Enregistrer
Partager
Nouvelle règle d'alerte
Exporter
Tables
Requêtes
Rechercher
Filtrer
Regrouper par : Sol...
Tout réduire
Favoris
Vous pouvez ajouter des favoris en cliquant sur l' ☆ icône
DNS Analytics (Preview)
LogManagement
Microsoft Sentinel
SecurityCenterFree
Journaux personnalisés
MQ_Early_Errologs_CL
MQ_Errorlogs_CL
Computer (string)
RawData (string)
TimeGenerated (datetime)
Type (string)
_ResourceId (string)
_SubscriptionId (string)
MQ_Events_CL
1 MQ_Errorlogs_CL ;
Résultats
Graphique
RawData
Type
TenantId
{"ibm_messageId":"AMQ9208E","ibm_arithInsert1":10054,"ibm_arithInsert2":10054,"ibm_comme...
MQ_Errorlogs...
1dded03a-dd57-41ad-93c2-fead0ebc8cf0
{"ibm_messageId":"AMQ9999E","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1"...
{"ibm_messageId":"AMQ9002I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
{"ibm_messageId":"AMQ9299I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
{"ibm_messageId":"AMQ9208E","ibm_arithInsert1":10054,"ibm_arithInsert2":10054,"ibm_comme...
{"ibm_messageId":"AMQ9999E","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1"...
{"ibm_messageId":"AMQ9002I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
{"ibm_messageId":"AMQ9299I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
{"ibm_messageId":"AMQ7467I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
{"ibm_messageId":"AMQ7468I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
{"ibm_messageId":"AMQ7467I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
{"ibm_messageId":"AMQ7468I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
{"ibm_messageId":"AMQ7467I","ibm_arithInsert1":0,"ibm_arithInsert2":0,"ibm_commentInsert1":...
Columns



```
MQ_Events_CL
```

	Type	TenantId
"eventType" : { "name" : "Queue Mgr Event", "value" : 44 }, "eventReason" : { "name" : "Queue Mgr Not Active", "value" : 2223 }, "...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Queue Mgr Event", "value" : 44 }, "eventReason" : { "name" : "Queue Mgr Not Active", "value" : 2223 }, "...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Logger Event", "value" : 91 }, "eventReason" : { "name" : "Logger Status", "value" : 2411 }, "eventCreatio...	MQ_Events_CL	1dded03a-dd5
"eventType" : { "name" : "Queue Mgr Event", "value" : 44 }, "eventReason" : { "name" : "Queue Mgr Not Active", "value" : 2223 }, "...	MQ_Events_CL	1dded03a-dd5



```
. "eventType" : { "name" : "Queue Mgr Event", "value" : 44 }, "eventReason" : { "name" : "Queue Mgr Not Active", "value" : 2223
. "eventType" : { "name" : "Queue Mgr Event", "value" : 44 }, "eventReason" : { "name" : "Queue Mgr Not Active", "value" : 2223
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "event
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "event
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "event
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "event
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "event
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "event
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "event
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...    MQ_Events_CL    1dded03a-dd5
. "eventType" : { "name" : "Command Event", "value" : 99 }, "eventReason" : { "name" : "Command PCF", "value" : 2413 }, "eventCr...    MQ_Events_CL    1dded03a-dd5
. "eventType" : { "name" : "Logger Event", "value" : 91 }, "eventReason" : { "name" : "Logger Status", "value" : 2411 }, "eventCreatio...    MQ_Events_CL    1dded03a-dd5
. "eventType" : { "name" : "Queue Mgr Event", "value" : 44 }, "eventReason" : { "name" : "Queue Mgr Not Active", "value" : 2223 }, "...    MQ_Events_CL    1dded03a-dd5
```

Next Steps

- Valider le fonctionnement
  - Complétude des évènements capturés
  - Purge des logs
  - …
- Créer des requêtes d'extraction côté Sentinel
- Alimenter un SIEM (Security Information & Event Management) avec alerting sur situation anormale

Merci de votre attention