MQ Command

DISPLAY QUEUE

DISPLAY QSTATUS

DISPLAY QMSTATUS

DISPLAY SBSTATUS

DISPLAY SVSTATUS --> We are not using any custom defined services.

2.1.1 ----> DISPLAY QSTATUS : Real time monitoring should be activate

Risk / Impact

Monitoring can be used in the following tasks:

Real time logs help to understand the steady state of the WebSphere MQ system. This helps with problem diagnosis if a problem occurs in the system.

And determining the condition of your queue manager at any moment and determining the cause of a problem in your system

To be checked :

The queue can be monitored by issuing commands to ensure that the queue is being serviced properly.

The channel can be monitored by issuing commands to ensure that the channel is running properly.

----------------DISPLAY QSTATUS---------------

DISPLAY QSTATUS(MWPRQM6) MONITOR

AMQ8450: Display queue status details.

QUEUE(MWPRQM6) TYPE(QUEUE)

CURDEPTH(0) LGETDATE( )

LGETTIME( ) LPUTDATE( )

LPUTTIME( ) MONQ(OFF)

MSGAGE( ) QTIME( , )

--------------------------------------------------------------------------------------------------------------------------------------------------------

2.1.2 -----> DISPLAY TRACE : Event Monitoring should be enabled --> We will enable trace at the time of troublshooting of issues.

Enforcing logging of events allows security incidents to be detected and help provide evidence to be available for analysis of those incidents.

Insufficient logging will result in a lack of an audit trail in the event of an unauthorized access or security breach

------------DISPLAY TRACE-------------------------------(NIRANJAN)

-bash-4.2$ strmqtrc -s

Trace [OFF]

Used slots [0 of 15]

Master Seq [1]

Current Time [1494390101]

Installation name [Installation1]

Installation id [1]

Data path [/var/mqm]

Binary Trace [ON]

EarlyTrace [OFF]

TimedTrace [OFF]

TraceUserData [-2]

MaxSize (Mb) [unlimited]

Trace Type [classic]

----------------------------------------------------------

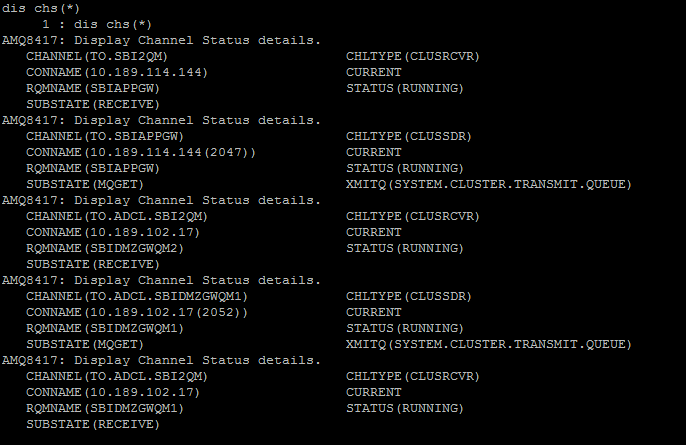
2.1.3 ----> DISPLAY LOG : Adequate space should be allocated for log files --> QMGR logs directory

If events are overwritten before they may be reviewed, an increased risk exists where continuous unauthorized activity may go undetected.

2.2.1 ----> DISPLAY SECURITY : Network Configuration : Access to the MQIPT configuration should be restricted

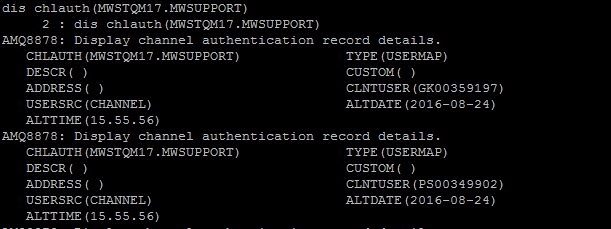
A user could attempt to identify and access MQ resources on any server listening with MQ services on TCP port. --> We are not using this functionality.

2.2.2 ---> DISPLAY CHSTATUS



2.3.1 ----> DISPLAY AUTHINFO --> We are not using this functionality.

2.3.1 ---> DISPLAY CHLAUTH



2.3.2 ---> MQ key repositories should be protected : Ensure that only the intended user can access the key repository file.

To Be checked :

Check the file permissions of key repository files and make sure that the files and containing folder are not world readable, preferably not even group readable. --> We have limited the access of MQ keys with proper file permissions. It will be accessed only by MQ admin user.

**<Please take the screen shot of “ssl” folder>**

2.4.1 & 2.4.2 ---->> DISPLAY CONN

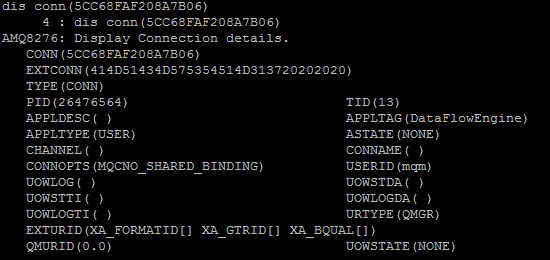
The SYSTEM.AUTO.SVRCONN channel is configured to allow anonymous connections.

An unauthorized user can trivially identify and use this default channel to enumerate MQ servers and queue manager names.

Once queue manager names are obtained, it may be possible to access their queues.

In addition, if the MCAUSER attribute is not set, the user can supply their own access authority over the channel.

This can give even legitimate users excessive privileges on queue mangers and queues.



2.4.3 ---> Message in default queues should be secured :

These queues, combined with default channels, allow an anonymous user to enumerate the names of nondefault channels.

This could allow an unauthorized user to identify channel names that are in common between production and non-production MQ environments,

and gain access to sensitive resources. **--> We are not using any default queues in our application.**

2.4.4 --->> SNMP should be secured : **--> To be addressed by Network Team.**

A UNIX system provides system information when queried using a default Simple Network Management Protocol (SNMP) string.

2.4.5 --->> Login banner should be enabled: It is possible to obtain a banner that identifies the version of the MQIPT server.

Network service details enable an attacker to target configuration defaults and software vulnerabilities. --> We are not displaying any information in login banner.

2.4.6 ---->Unnecessary files and services should be cleared **--> We are doing housekeeping activites regurlarly.**

Unnecessary files and folders should be cleared from the production web servers

2.5.1 & 2.5.2

Admin should be member of the MQ group **--> It is already implemented. mqm user is a part of mqm group.**

WebSphere MQ administrator, must be a member of a special group called the mqm group

Users in the mqm group are granted full administrative privileges over WebSphere MQ. For this reason,

you should not enrol applications and ordinary users in the mqm group.

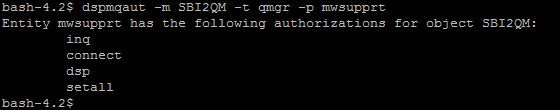
The mqm group should contain the accounts of the WebSphere MQ administrators only.



2.5.3 ---> Command server should to be secured :The Command Server should not accept commands through default channels.

An unauthorized user on the network can anonymously issue commands to the MQ server, including listing all queue names and channels.

The Command Server also allows a remote user to start and stop the queue manager and create MQ object **--> Command server and QMGR is always secured by using chlauth and qmgr authentications.**

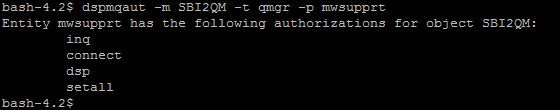


2.5.4 ---->> Queue manager access should be restricted.It is possible to view,

add or edit messages on any queue for which a user knows the name and a channel with which to access its queue manager.

An unauthorized user could gain access to potentially sensitive information on queues, including modifying the data.

An unauthorized user could also remove logging data from queues in order to cover their tracks. **--> Using channel auth and qmgr auth, the access to qmgr is limited to specific users.**



2.5.5 ----->> Session level cryptography should be enabled. **--> To be discussed after MQ migration.**

Session level cryptography encrypts and decrypts session data using the DES algorithm.

For IBM MQ system the mandatory encryption should be enabled for a session using strong encrypted algorithm.