IBM MQ Appliance

What’s new in 2017 and futures

Important Disclaimers

IBM's statements regarding its plans, directions and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Important Disclaimers

- **IBM Confidential**. Unless specifically advised otherwise, you should assume that all the information in this presentation (whether given in writing or orally) is IBM Confidential and restrict access to this information in accordance with the confidentiality terms in place between your organization and IBM.
- **Content Authority**. The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided AS-IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.
- **Performance**. Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
- **Customer Examples**. Any customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.
- **Availability**. References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates.

Trademark acknowledgements

•IBM, the IBM logo etc. are trademarks of International Business Machines Corporation, registered in many jurisdictions.

•Other company, product and service names may be trademarks, registered marks or service marks of their respective owners. A current list of IBM trademarks is available on the web at "Copyright and trademark information" ibm.com/legal/copytrade.shtml

Agenda

- Introduction
- V9.0.1
  - New UI
  - HA Floating IP support
  - Queue manager backup/restore and automatic start-up
  - RESTful administration, administrative security, SNMP
- V9.0.2
  - MQ REST API, HA SSH key renewal
- V9.0.3
  - AMS MCA interception
- V9.0.4
  - SAN support
- Futures

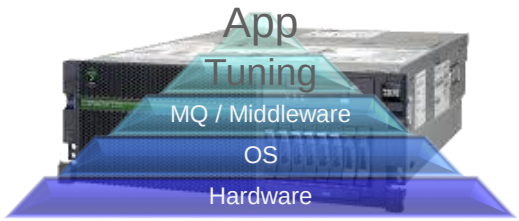
What's an MQ Appliance?

- The scalability and security of IBM MQ
- Integrates seamlessly into MQ networks and clusters
  - Familiar administration model for administrators with MQ skills
- The convenience, fast time-to-value and low total cost of ownership of an appliance
- Ideal for use as a messaging hub running queue managers accessed by clients, or to extend MQ connectivity to a remote location
- Familiar feel for existing MQ users – application interfaces, administration, networking/clustering, security….
- Plus new appliance specific features – e.g. built in high availability

Key differences with appliance form-factor

IBM MQ Appliance

- Prebuilt for hub pattern – no apps on device
- No additional software installation
  - No user exits in MQ
  - Monitoring agents must be remote
- High availability out-of-the-box
- Pre-tuned
- Single firmware update for whole appliance
  - Firmware update inc. appliance and MQ fix pack
  - Can be rolled back as an single unit



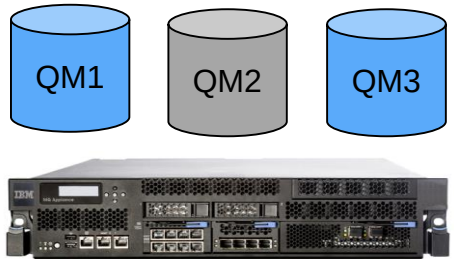
IBM MQ on custom server

- DIY hub or generic server – apps + middleware
- Install any software
  - Build & maintain your own custom extensions
  - Add local monitoring agents
- Needs HA cluster SW or network storage for HA
- Custom tuning for each layer (OS/middleware)
- Discrete maintenance for each layer
  - MQ fix packs
  - OS maintenance, security patches, etc.

IBM MQ Appliance V8.0 (recap)

- Announced in February 2015 – GA was 13 March 2015 (M2000)
- High availability (HA) support built in
- Firmware updates delivered new function:
  - 8.0.0.4 (October 2015)
    - Disaster recovery (asynchronous replication) for single appliances
  - 8.0.0.5 (May 2016)
    - Disaster recovery for HA groups
    - AMQP channels for MQ Light applications
    - Support for the M2001 hardware model
      - SSD disks and 4-port 10Gb Ethernet module
- V8.0 is now provided as the long-term support (LTS) firmware version

High availability – concept

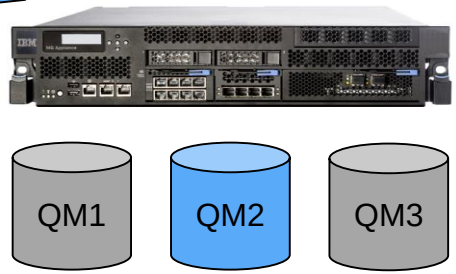


No persistent data loss on failure

No external storage

No additional skills required

Fully synchronous replication

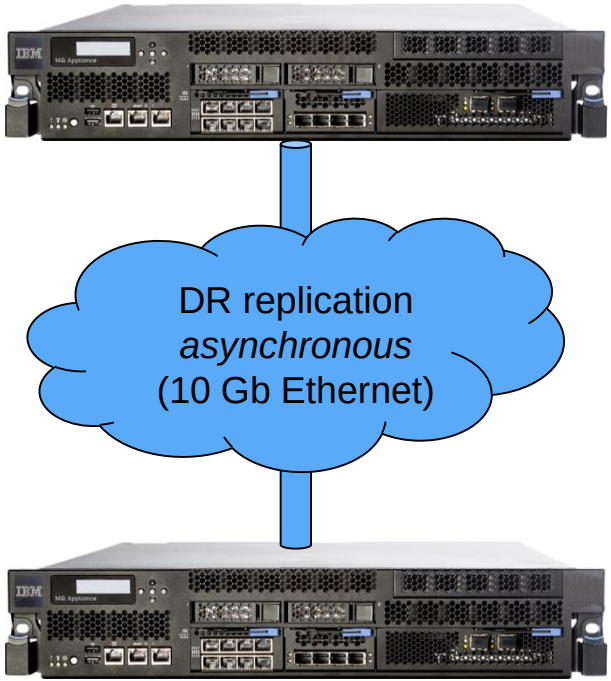


Manual control of failover for migration/maintenance

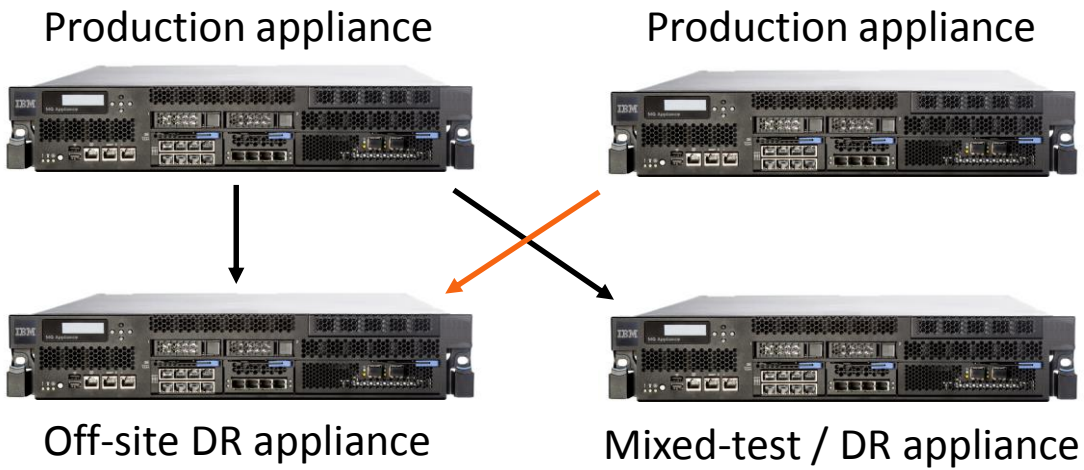
Queue manager level active/passive (i.e. both appliances can run workload)

Disaster recovery (8.0.0.4) – concept

- Provides for longer distance recovery than HA
  - e.g. out-of-region standby site
- Still ultimately requires high bandwidth connectivity as all persistent data is fully mirrored
- But - asynchronous so better choice than HA for higher latency, ‘bursty’ or ‘lossy’ networks
  - Means most recent messages are potentially lost on fail-over and application logic must consider this
- Manual interaction required to trigger fail-over / fail-back



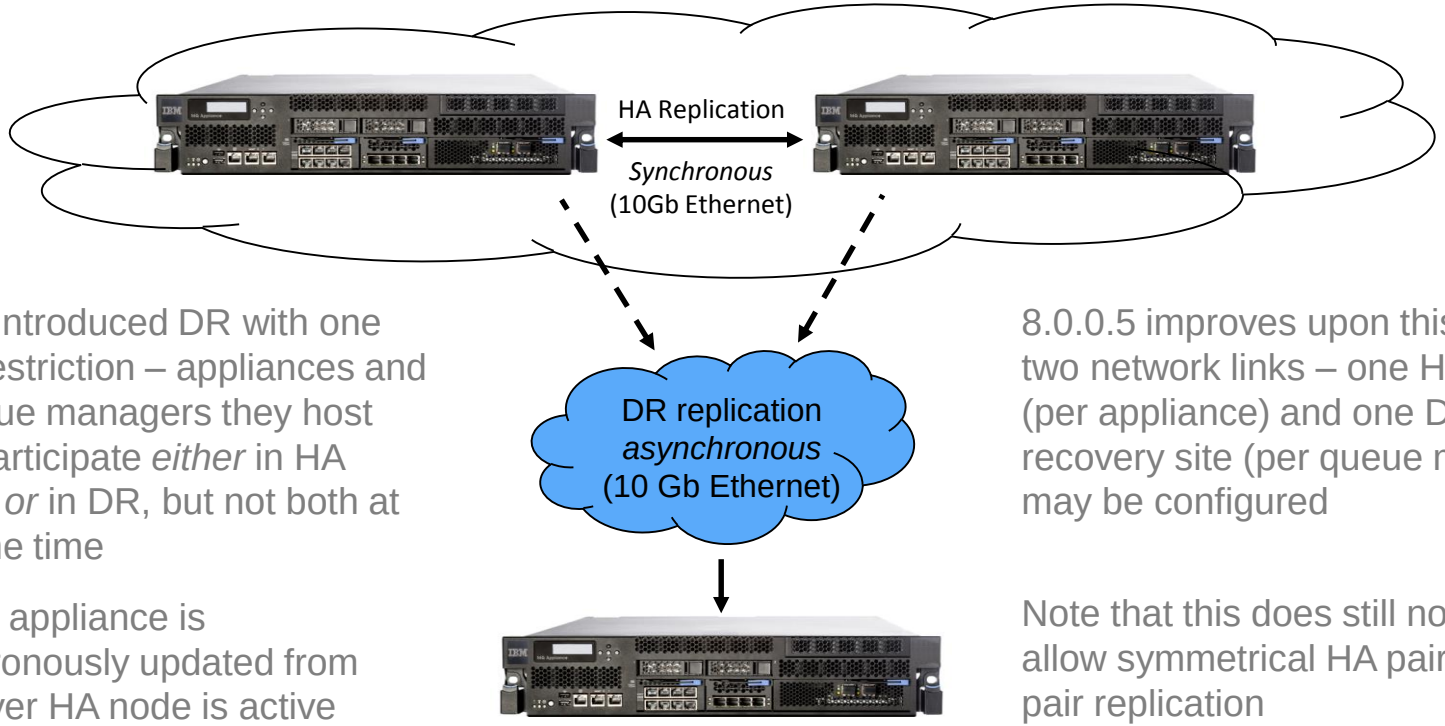
Disaster recovery – flexible topologies



Flexible configuration:

- As with HA, configuration is per queue manager – though with DR there is no concept of a ‘group’
- Each QM independently configures replication to one other appliance
- For example, could configure single ‘DR’ site covering live appliances at multiple sites

Disaster recovery for HA groups (8.0.0.5)



8.0.0.4 introduced DR with one major restriction – appliances and the queue managers they host could participate *either* in HA groups, *or* in DR, but not both at the same time

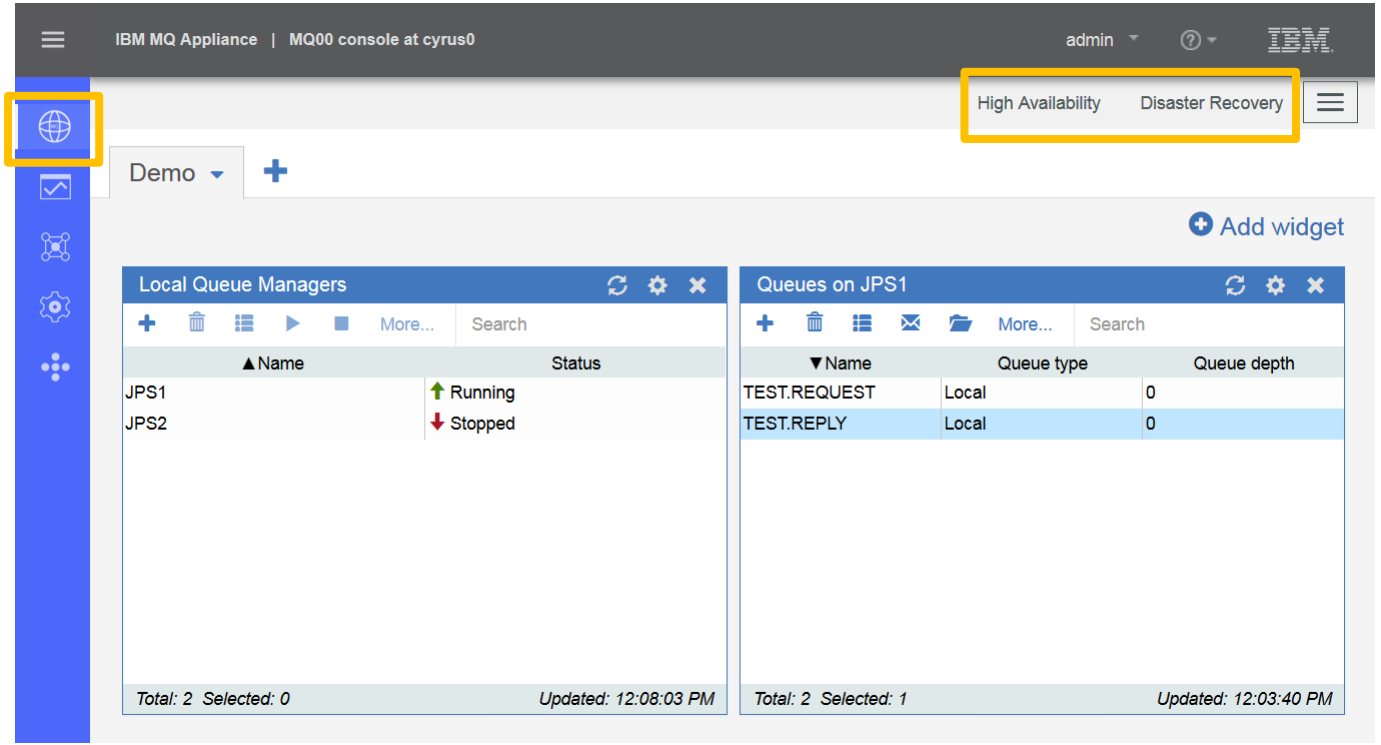
The DR appliance is asynchronously updated from whichever HA node is active

8.0.0.5 improves upon this using two network links – one HA partner (per appliance) and one DR recovery site (per queue manager) may be configured

Note that this does still not (yet) allow symmetrical HA pair to HA pair replication

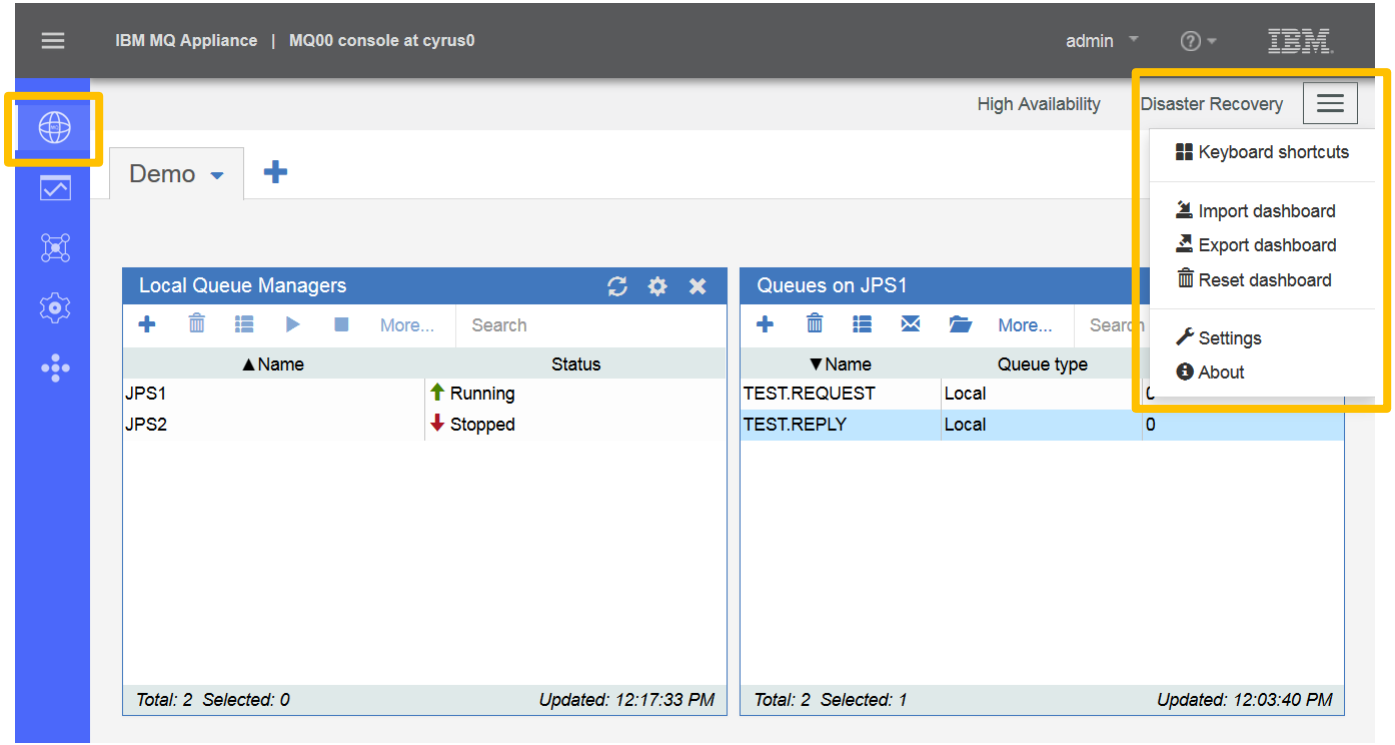
New web UI (9.0.1)

- Embedded MQ Console
- Easy access to configure high availability and disaster recovery



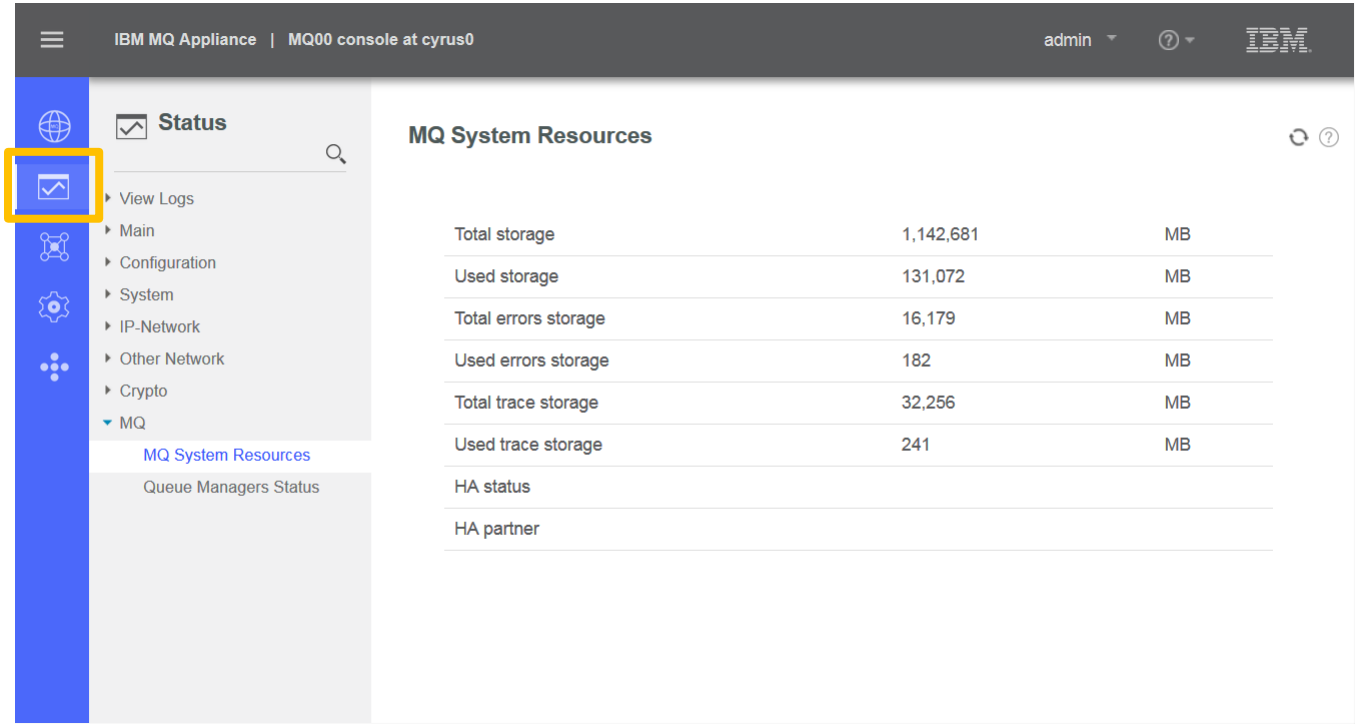
New web UI (9.0.1)

- Options to import, export and reset the MQ Console dashboard
- Ideal for replicating between appliances



New web UI (9.0.1)

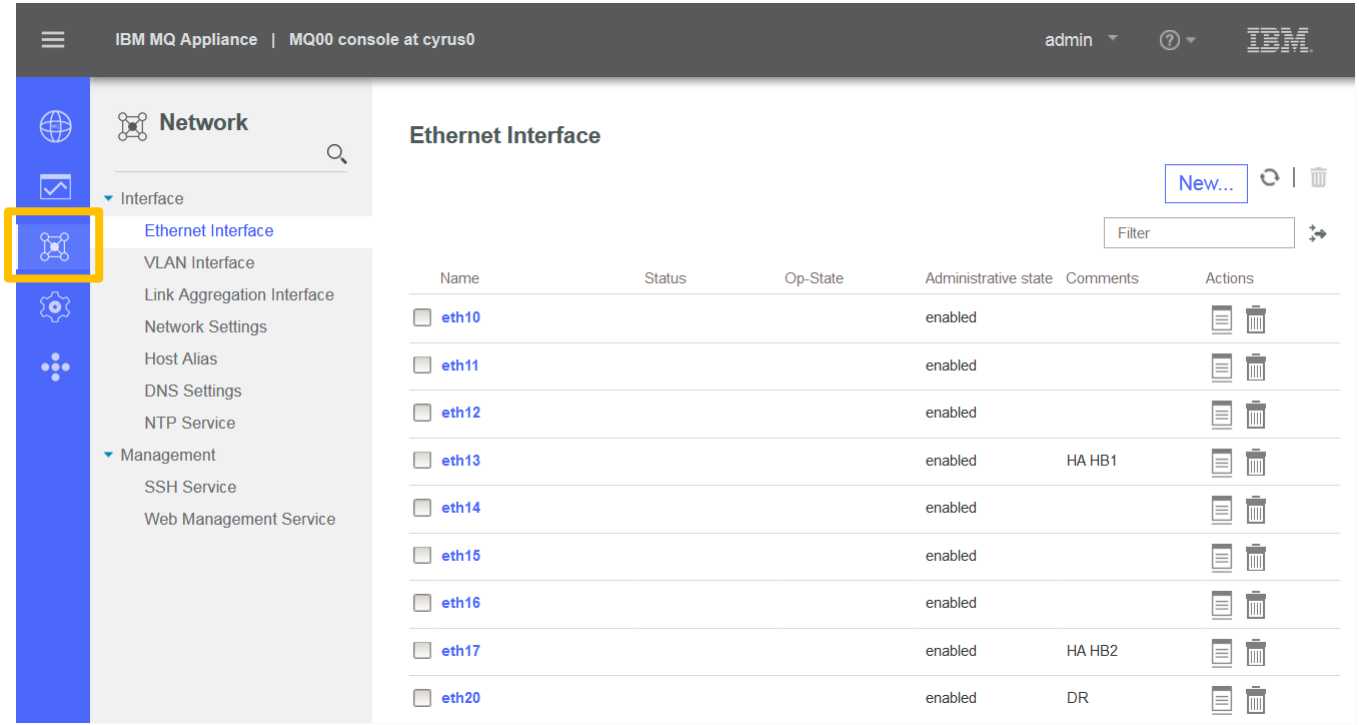
- View status information about resources, hardware sensors, networking, active users, system logs and more



System resource example for a M2000 appliance – the M2001 has 3TB of storage

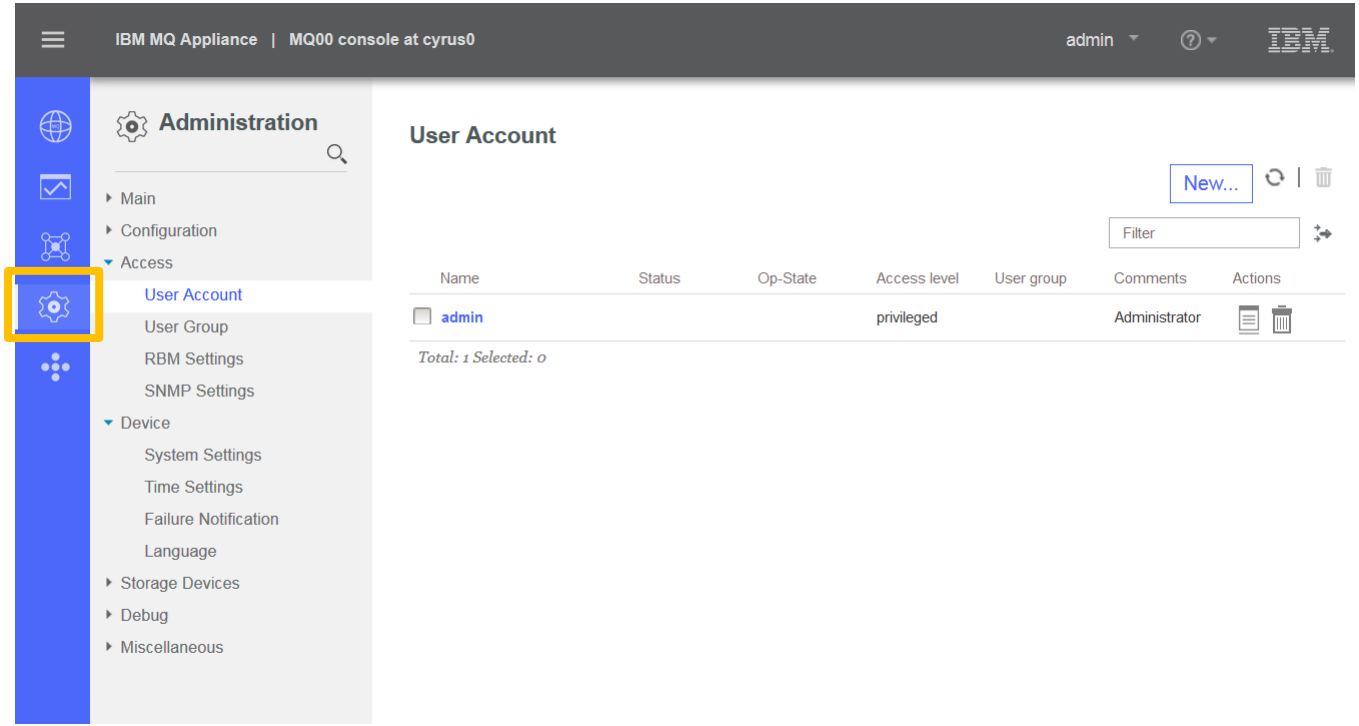
New web UI (9.0.1)

- Configure the Ethernet interfaces, VLANs, link aggregation and other network settings
- Configure SSH and the web UI



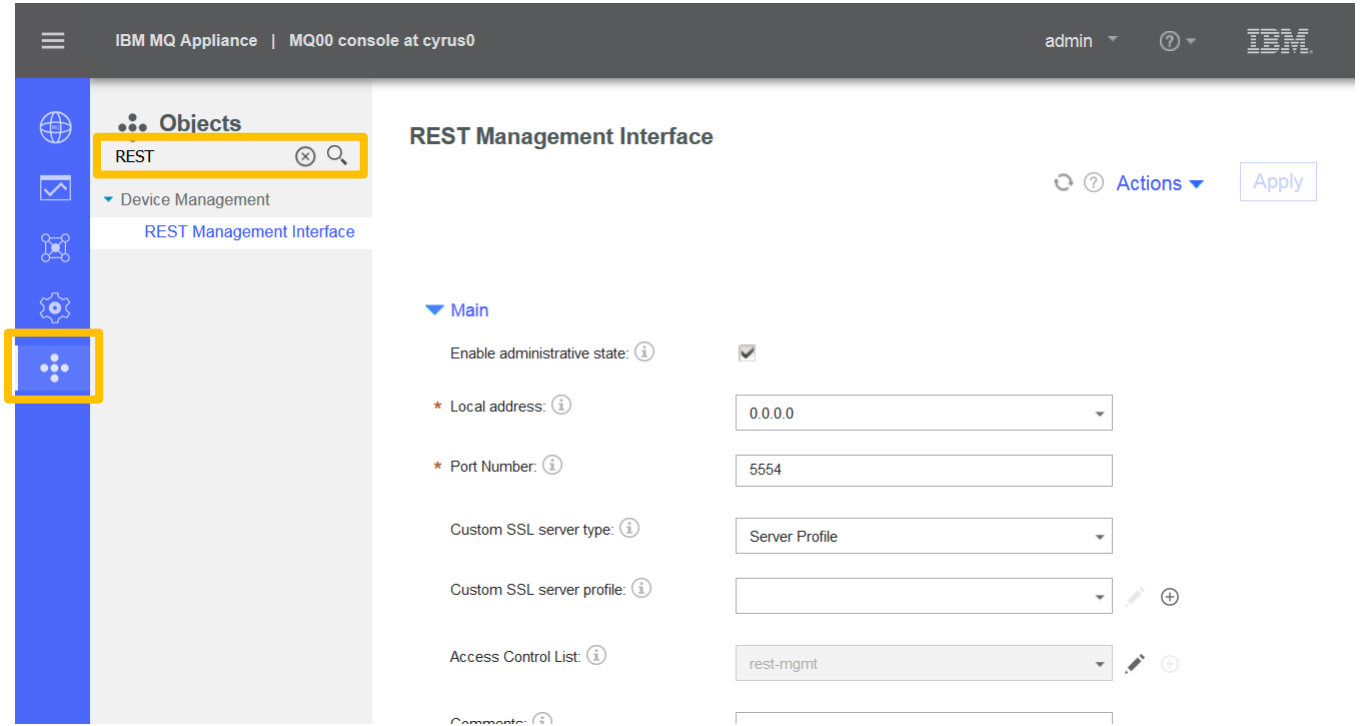
New web UI (9.0.1)

- Administer local user accounts, role-based management (RBM), SNMP and other system settings



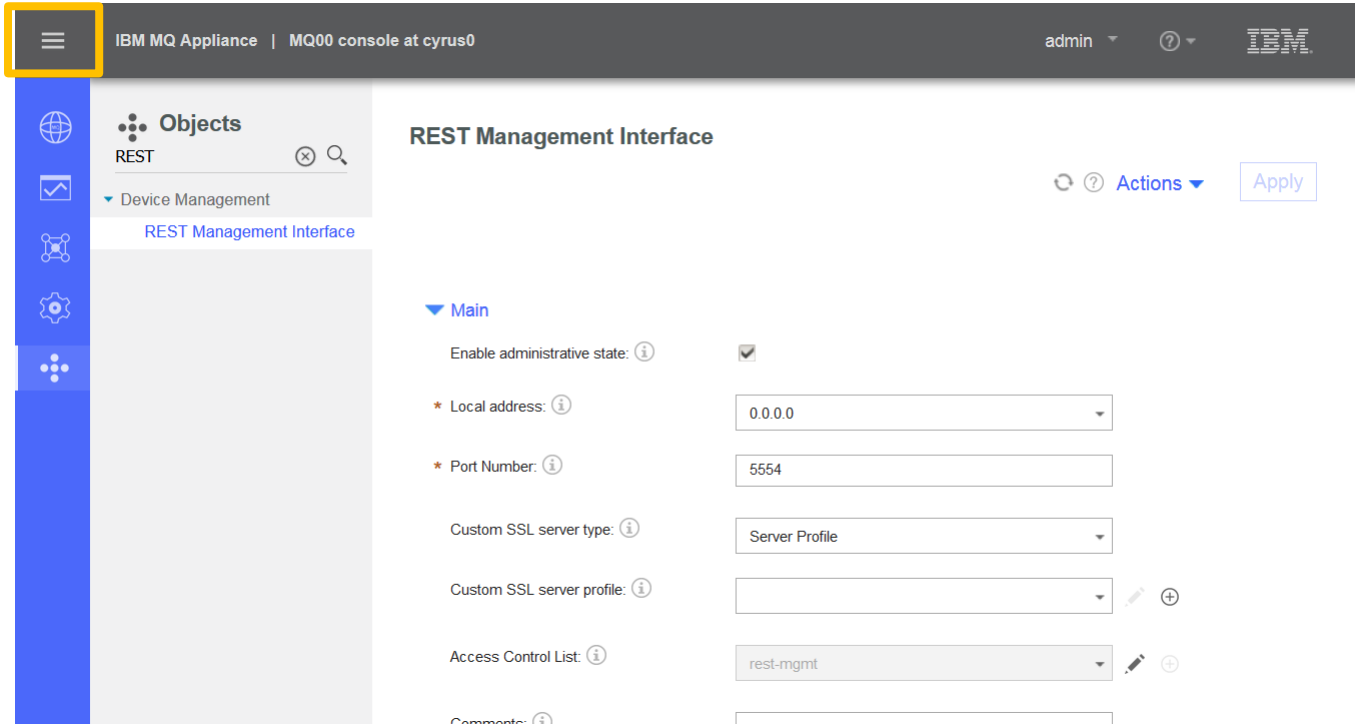
New web UI (9.0.1)

- Manage all system objects in a single view
- Search for object types using keywords



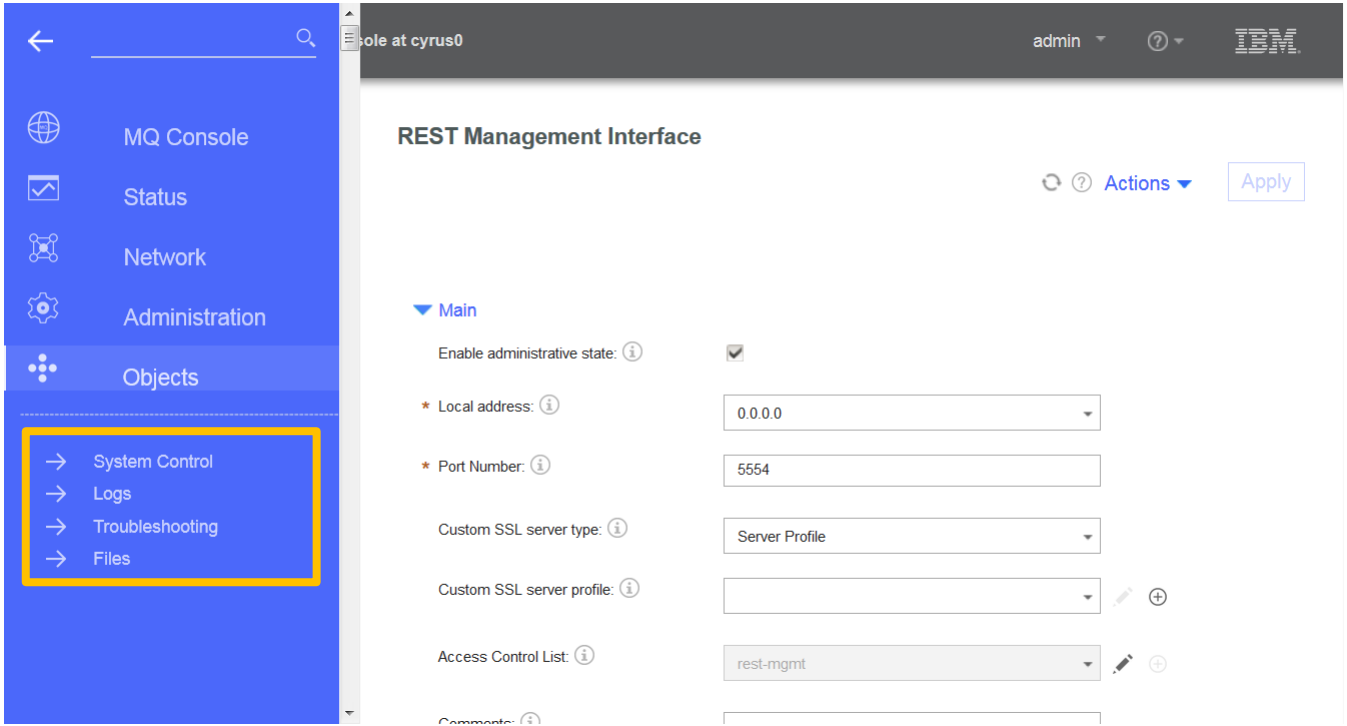
New web UI (9.0.1)

- Expand the searchable navigation menu for quick access to common items



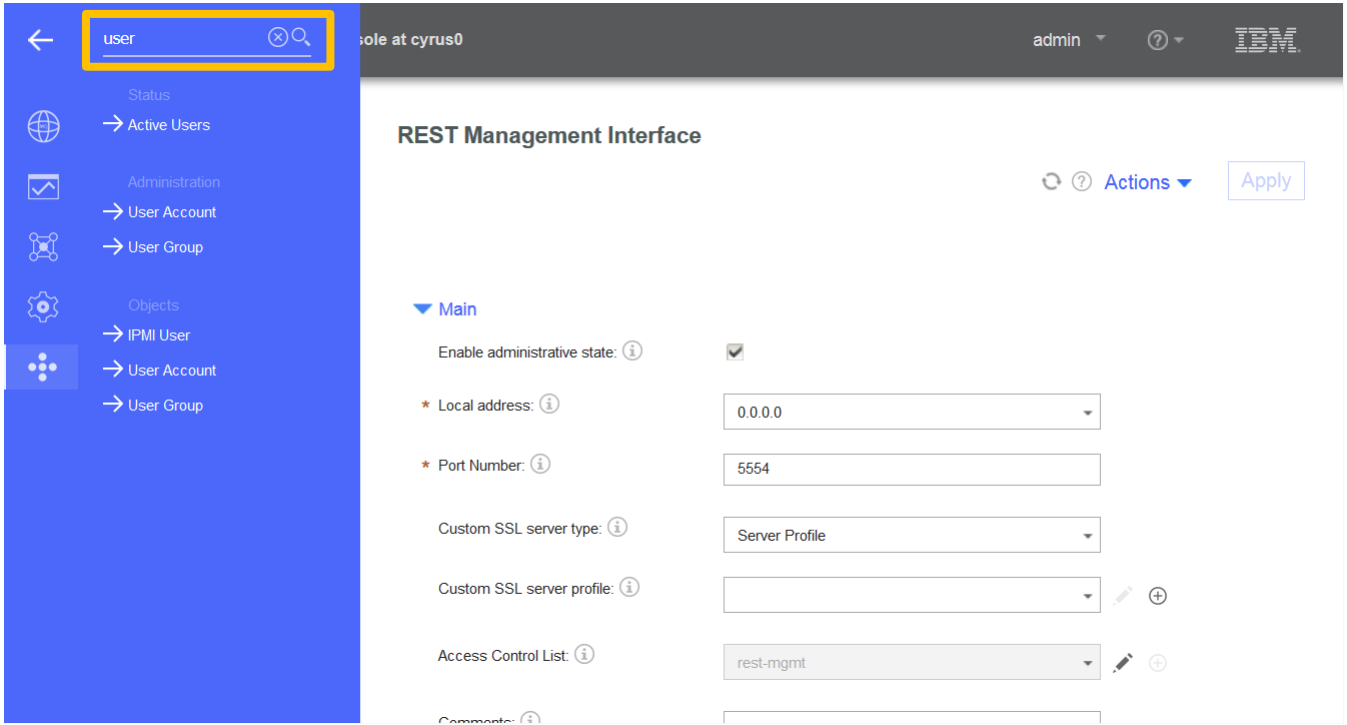
New web UI (9.0.1)

- Access system logs and files at the click of a button



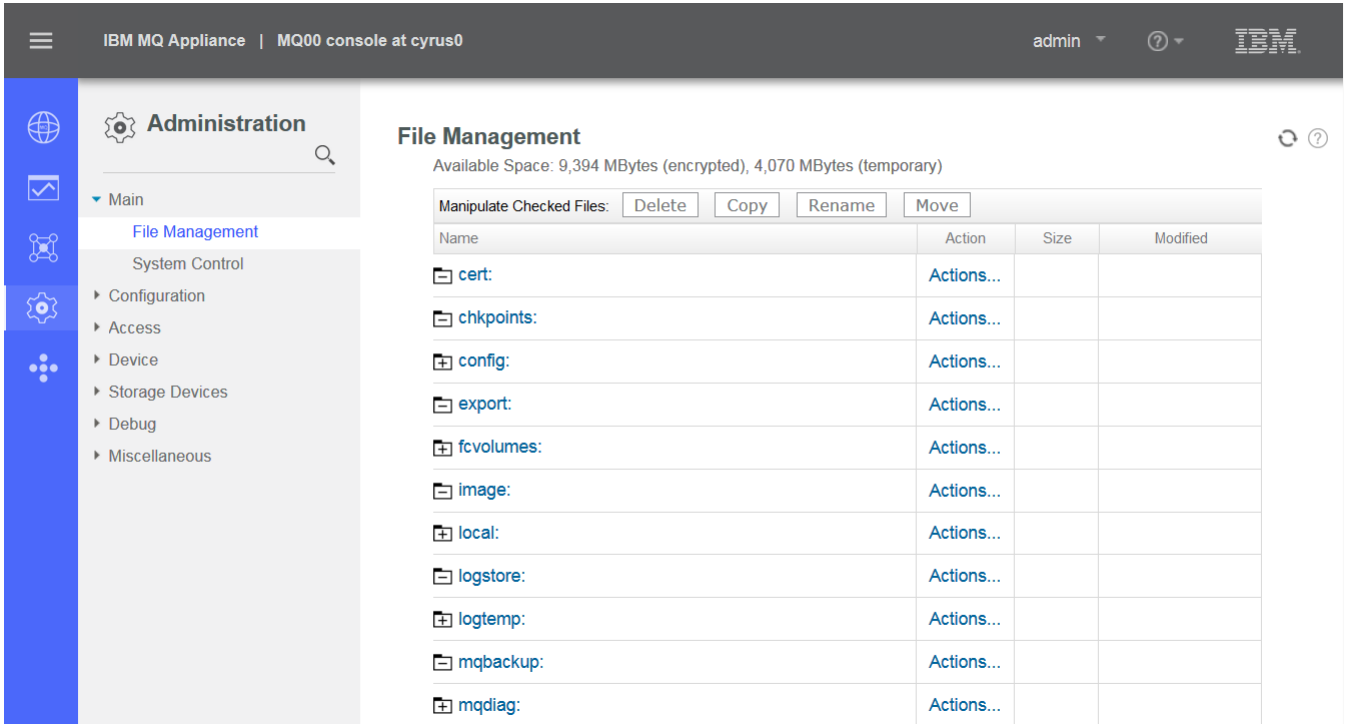
New web UI (9.0.1)

- Use keywords to search for relevant information throughout the UI



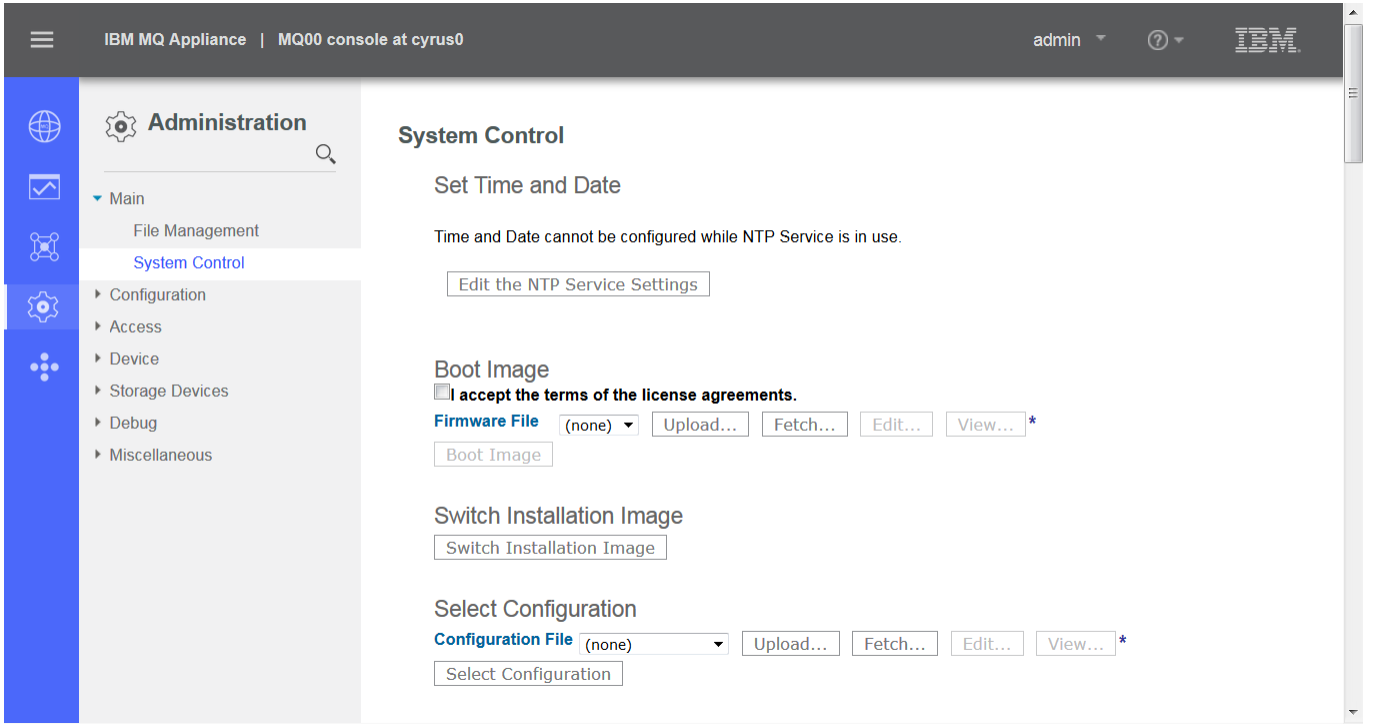
New web UI (9.0.1)

- Upload, download and manage local files, such as logs, trace and certificates

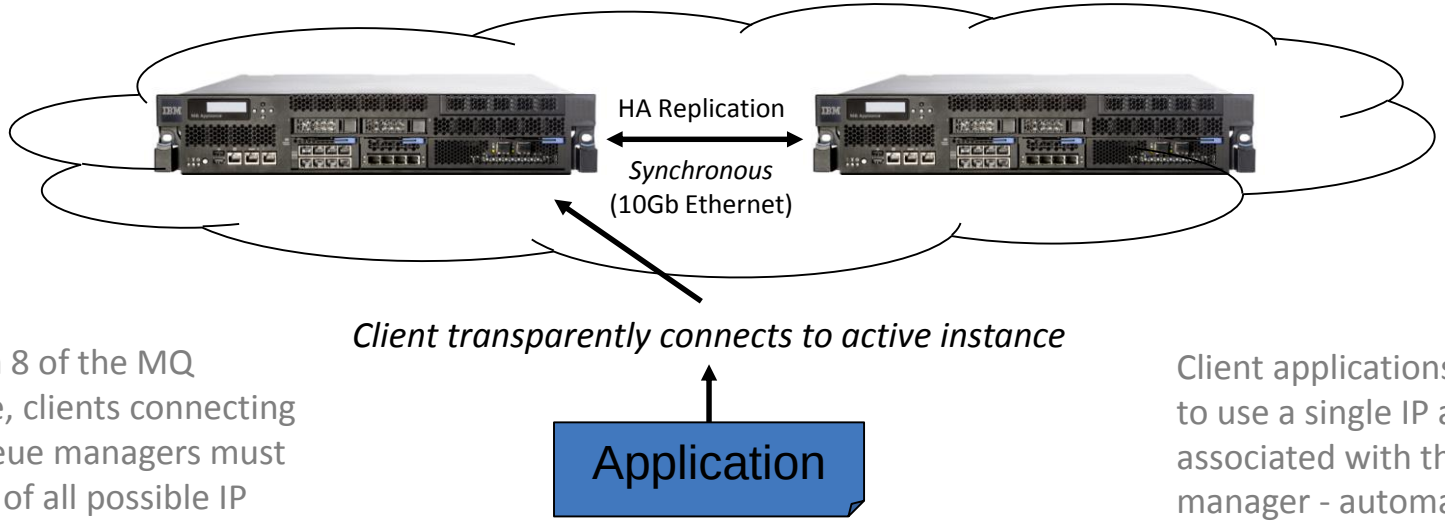


New web UI (9.0.1)

- Use System Control to:
  - Apply firmware updates
  - Shutdown or reboot the appliance
  - Change the logged in user's password (if applicable)
  - Control the blue locator LED



High availability – floating IP support (9.0.1)



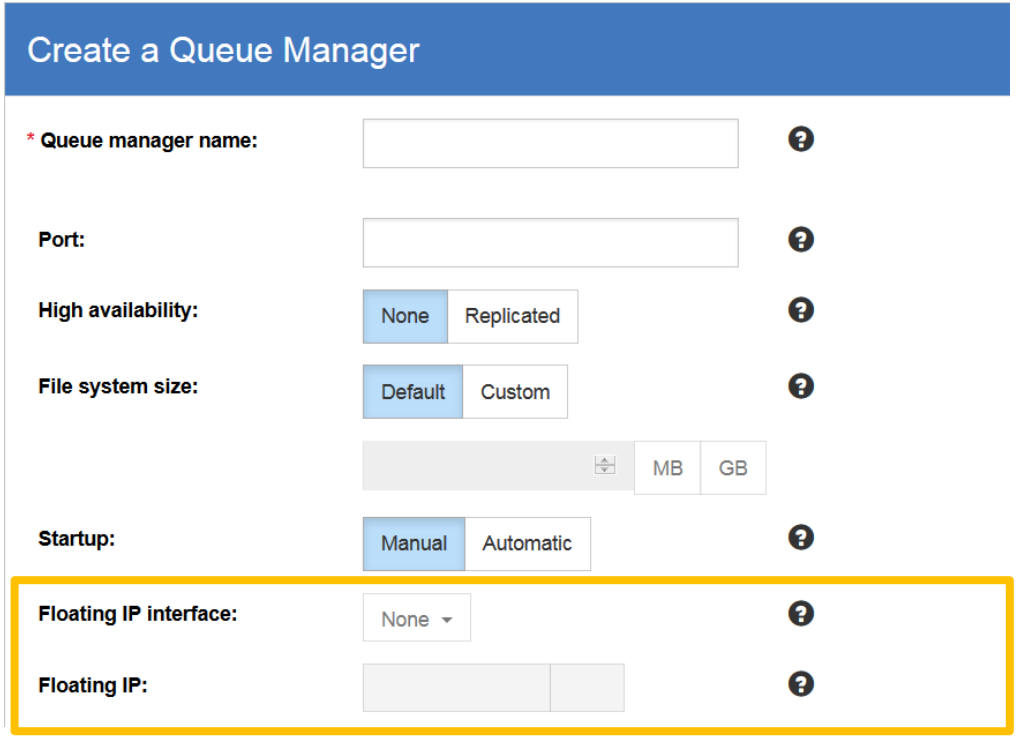
In version 8 of the MQ Appliance, clients connecting to HA queue managers must be aware of all possible IP addresses (e.g. via comma separated list or CCDT)

Particularly useful when replacing existing standalone queue managers with HA Appliance queue managers, requiring no changes on the application side

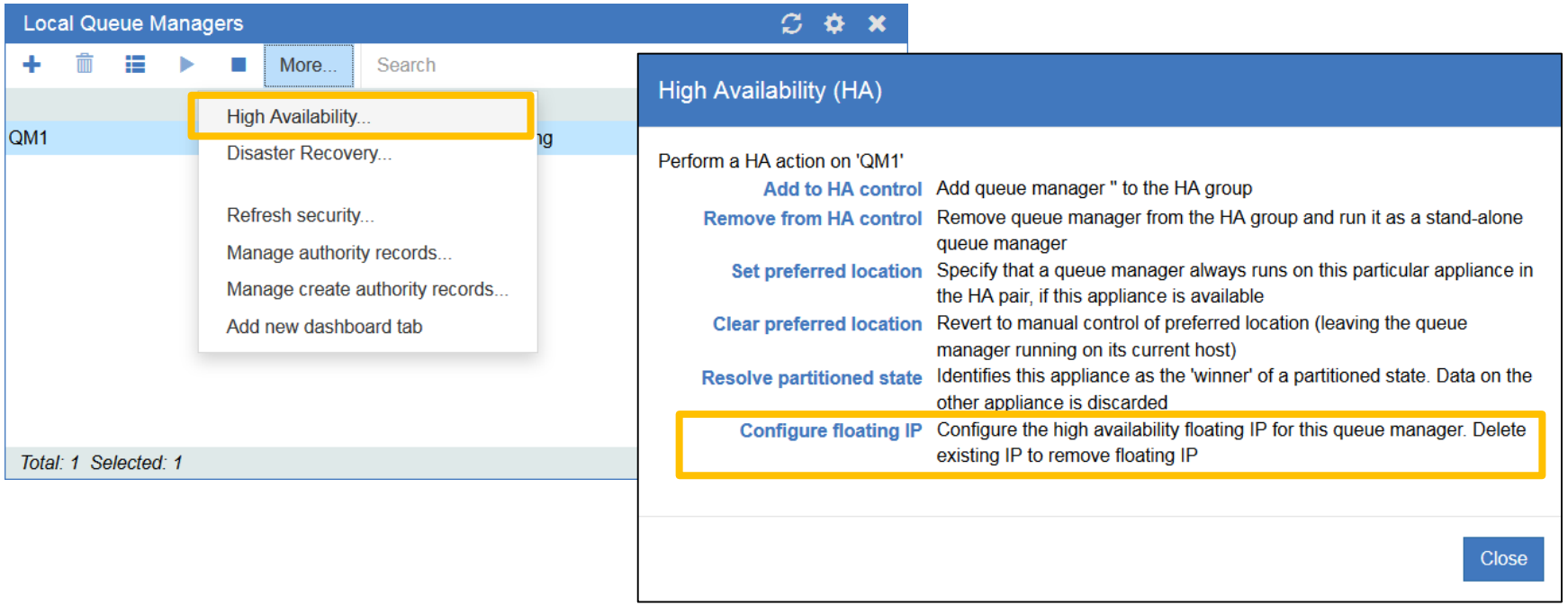
Client applications now able to use a single IP address associated with the queue manager - automatically adopted by whichever instance is currently active

Floating IP configuration (web UI)

- Option to configure the floating IP at queue manager creation in the web UI …



Floating IP configuration (web UI)



… and for existing queue managers

Floating IP configuration (CLI)

- A new **sethaint** command can be used to configure a HA floating IP address for a queue manager
- The **dspmq** command has been updated to display the IP information

```
mqa(mqcli)# sethaint -m HA1 -a -f 9.20.87.200 -l eth10
The sethaint command succeeded.

mqa(mqcli)# dspmq -o ha
QMNAME(HA1)       HA(Replicated) HALSADDR(9.20.87.200) HALSINT(eth10)
```

- Define a listener to use the floating IP for inbound connections
  - `DEFINE LISTENER(mylist) IPADDR(9.20.87.200)`
- Use LOCLADDR for outbound connections
  - `DEFINE CHANNEL(mysdr) CHLTYPE(SDR) LOCLADDR(9.20.87.200)`

Automatic queue manager start-up (9.0.1)

- New option to configure non-HA queue managers to be started automatically when the appliance boots (was already automatic for HA)
- Option to set in the create queue manager UI dialog:

- Use **dspmqini** and **setmqini** to query and modify using the CLI:

```
mqa(mqcli)# setmqini -m JPS1 -s InstanceData -k Startup -v Automatic
Key Startup was successfully updated in stanza InstanceData for
queue manager JPS1.

mqa(mqcli)# dspmqini -m JPS1 -s InstanceData -k Startup
Automatic
```

Queue manager backup/restore (9.0.1)

- New option to create a point-in-time backup for a queue manager
  - Provides a fall-back position should a firmware update need to be rolled back
  - Can also be used to move a queue manager from one appliance to another
- Allocate storage for backups:

```
mqa(mqcli)# createbackupfs -s 100G
The createbackupfs command succeeded.
```

- Use `mqbackup` and `mqrestore` to backup/restore queue managers:

```
mqa(mqcli)# mqbackup -m JPS3
Backup operation for 'JPS3' queue manager has completed successfully.
Created backup file: mqbackup:/QMgrs/JPS3.bak
```

Administrative security (9.0.1)

- Two distinct types of user on the appliance
  - Users who administer the system (appliance/administrative users)
  - Users who perform messaging operations (messaging users)

- Role-Based Management (RBM)
  - New security model for managing appliance users
  - More granular and flexible user and authority management
  - Core capabilities
    - User authentication
    - Credential mapping (authorisation)
    - Password and account policy

Administrative security (9.0.1)

- User authentication options
  - Local users (the only option available in version 8)
  - Users defined in an XML file
    - Easy central deployment of user credentials using SCP or REST
  - External LDAP repository
    - LDAP is commonly used to provide a single sign-on solution
      - E.g. OpenLDAP, Microsoft Active Directory and IBM Security Directory Server
    - Single control point, avoids bespoke security policy
    - Supports user authentication using any unique attribute in user profiles
      - E.g. Serial number, common name, email address
    - Supports LDAP and LDAPS (SSL/TLS) and load balancing for availability
    - Fallback users allow access when LDAP repository is unavailable or settings are wrong

Administrative security (9.0.1)

- Credential mapping
  - Policies assign authorities to users or groups (roles)
  - Generic or specific profiles define access to a type or class of resource
  - Can quickly define simple rules or build granular definitions for complex policies
  - Authority types:
    - View existing objects (read)
    - Edit existing objects (write)
    - Define a new object (add)
    - Remove an object (delete)
    - Perform related actions (execute)

Administrative security (9.0.1)

- Credential mapping cont…
  - Restrict access to specific interfaces
    - E.g. Require local access for more sensitive operations
  - Define access policies using local groups or an XML file
    - Optionally store user-group mapping in LDAP
  - Restrict access to administrative interfaces
    - Web UI, REST API, SSH
  - Can now grant access to system resources but not MQ (or vice-versa)
    - Access to MQ in the CLI is all or nothing
    - Access to MQ Console is as per other platforms (full admin, read-only admin, custom)

Administrative security (9.0.1)

- Password and account policy
  - Define policies for local users
    - Not applicable to XML file and LDAP authentication
  - Configure password rules
    - Minimum length, complexity, expiration, restrict reuse
  - Account policies
    - Restrict the built-in ‘admin’ account to the serial connection
    - Account lockout after excessive failed login attempts
      - Configurable lockout duration and attempt threshold
    - Disconnect idle CLI sessions

SNMP monitoring (9.0.1)

- Support for Simple Network Management Protocol
  - Supports SNMP versions 1, 2c, and 3
  - Configure an external SNMP server can collect status information
- Download enterprise MIBs that describe the SNMP interface
  - MIB stands for Management Information Base
  - One MIB for configuration, one for status and another for traps/notifications
- Receive notifications about system events
  - Respond to hardware failures, temperature alerts, network errors, …
  - MQ events are not currently supported

SNMP monitoring (9.0.1)

- Use SNMP tooling or commands
- Example to query the power supply electrical current:

```
$ snmptable -v 2c -c MQ cyrus0 mqStatusCurrentSensorsTable
SNMP table: IBM-MQ-APPLIANCE-STATUS-MIB::mqStatusCurrentSensorsTable

 mqStatusCurrentSensorsName mqStatusCurrentSensorsValue
mqStatusCurrentSensorsUpperCriticalThreshold
mqStatusCurrentSensorsReadingStatus
          Current PU +12V 1                          9200 mA
44800 mA                                  ok
           Current PU +3.3V                          2400 mA
16000 mA                                  ok
             Current PU +5V                          2400 mA
16000 mA                                  ok
```

SNMP monitoring (9.0.1)

Query queue manager status:

```
$ snmptable -v 2c -c MQ cyrus0 mqStatusQueueManagersStatusTable
SNMP table: IBM-MQ-APPLIANCE-STATUS-MIB::mqStatusQueueManagersStatusTable

 mqStatusQueueManagersStatusName mqStatusQueueManagersStatusStatus
mqStatusQueueManagersStatusCpuUsage mqStatusQueueManagersStatusUsedMemory
mqStatusQueueManagersStatusUsedFs mqStatusQueueManagersStatusTotalFs
mqStatusQueueManagersStatusHaRole mqStatusQueueManagersStatusHaStatus
                              JPS1                                 Running
0 %                                  177 MB                                 225 MB
32256 MB                                  NA
NA
                              JPS2                       Ended immediately
0 %                                    0 MB                                 229 MB
64512 MB                                  NA
NA
```

REST administration (9.0.1)

- REST management interface for system administration
- Query system resource status
  - `/mgmt/status/default/…`
- Configure system resources (users, networking, system settings, …)
  - `/mgmt/config/default/…`
- Perform actions (password resets, set log level, shutdown/reboot, …)
  - `/mgmt/actionqueue/default`
- Upload/download files
  - `/mgmt/filestore/…`
- Discover the REST API
  - `/mgmt/metadata/…` and `/mgmt/types/…`

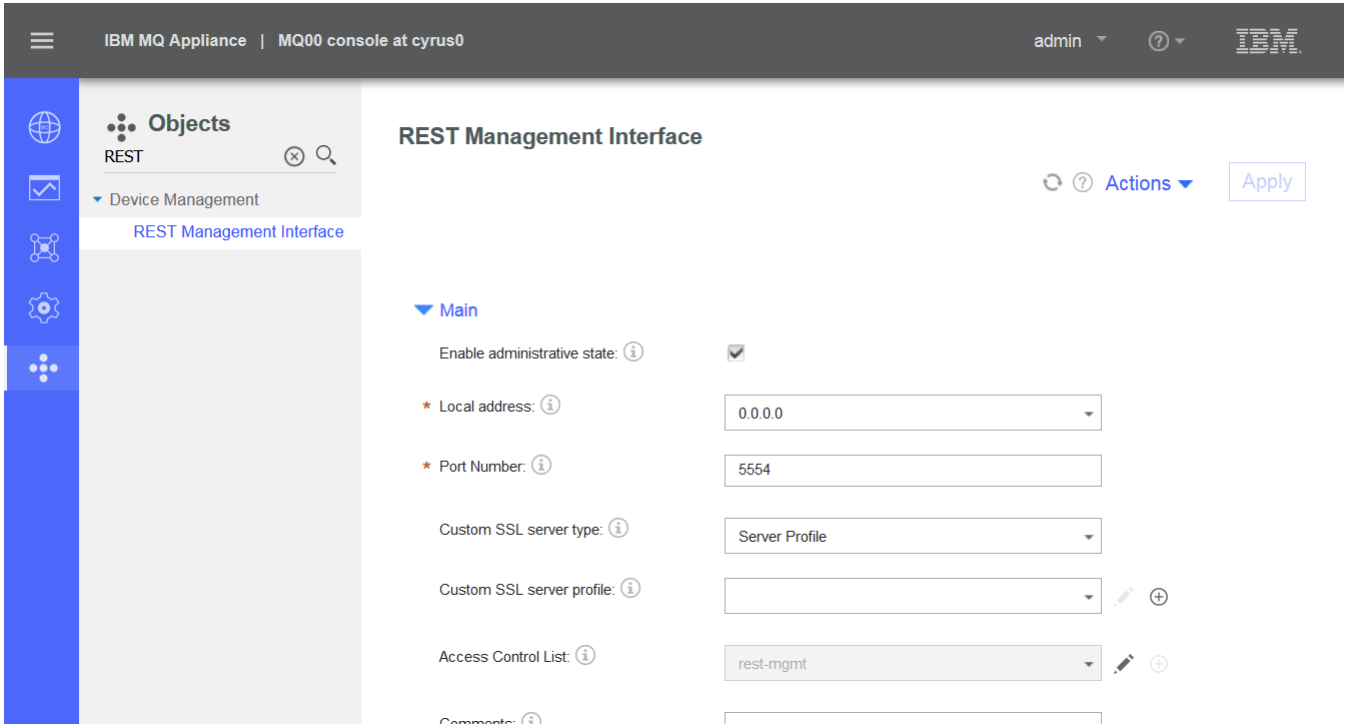
REST administration (9.0.1)

- Request methods:
  - GET – query status, object lists/definitions, download file, etc.
  - POST – create new objects, perform actions
  - PUT – create or update an object if it already exists
  - DELETE – delete objects
  - OPTIONS – query supported methods for a URI

- Use query parameters to customise the response:
  - `?view=recursive` - expand object references (nested objects)
  - `?depth=n` - limit the level of recursion
  - `?state=true` - query the runtime state of an object

REST administration (9.0.1)

- All system management REST requests use Basic Authentication (https)
- Enable/disable
- Configurable interface, port, SSL/TLS settings
- Restrict clients based on IP using access control lists



REST administration (9.0.1)

- Example:
  - GET `/mgmt/status/default/SystemMemoryStatus`
  - Response:

```
{
  "_links" : { … }
  "SystemMemoryStatus" : {
    "MemoryUsage" : 2,
    "TotalMemory" : 193638,
    "UsedMemory" : 3677,
    "FreeMemory" : 189961
  }
}
```

REST administration (9.0.1)

- Understand how to interpret the response:
  - GET `/mgmt/metadata/default/SystemMemoryStatus/MemoryUsage`
  - Response:

```
{
  "property" : {
    "name" : "MemoryUsage",
    "type" : { "href" : "/mgmt/types/default/dmUInt32“ },
    "display" : "Memory usage",
    "summary" : "The percentage of memory used.",
    "units" : "%",
    "description" : "The instantaneous memory usage as a
                     percentage of the total memory.“
  }
}
```

MQ REST API (9.0.2)

- MQ REST management API added to the appliance
  - Complements use of REST for system management
- Base URI: `https://<hostname>:<port>/ibmmq/rest/v1/`
- Enabled at the same time as the system management REST API
- No Liberty configuration required
  - Same user authority model and roles as the MQ Console
- Includes all URIs exposed on other platforms

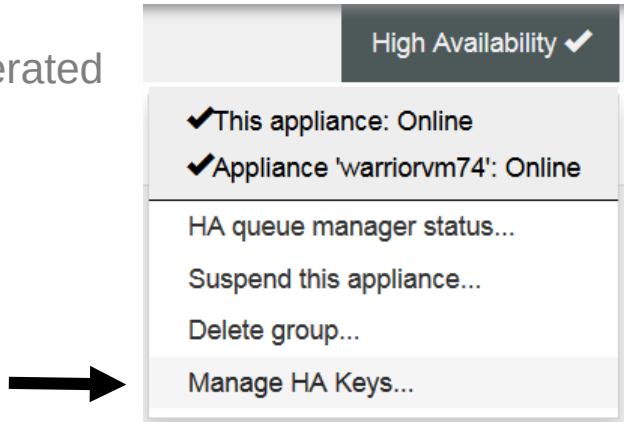
HA SSH key renewal (9.0.2)

- Appliances in a HA group use SSH keys for internal communication
  - Keys not exposed to users
  - Security best practice recommends periodically regenerating SSH keys
  - New capability introduced to allow administrators to do this (undisruptive)
- Two new commands (and equivalent UI capability):
  - `crthakeys`: Regenerates the SSH keys
  - `dsphakeys`: Displays when the SSH keys were last generated

```
mqa(mqcli)# crthakeys
The crthakeys command succeeded.

mqa(mqcli)# dsphakeys
SSH key generation time: 2017-02-13 16:47:55
```

The generation time is blank if generated at 9.0.1 or earlier



AMS MCA Interception (9.0.3)

- Offers parity of function with software MQ
- Queue manager can perform AMS digital signing and/or cryptographic operations on behalf of client applications
- Configured per server-connection channel using **setamschl** / **dspamschl**
  - Always use SSL/TLS channels – AMS policies applied on queue manager entry/exit
- Use cases:
  - For clients that are not AMS-capable (e.g. Message Service client for .NET)
  - When it is not practical to configure AMS for each client instance
    - For example, 1000s of clients

AMS MCA Interception (9.0.3)

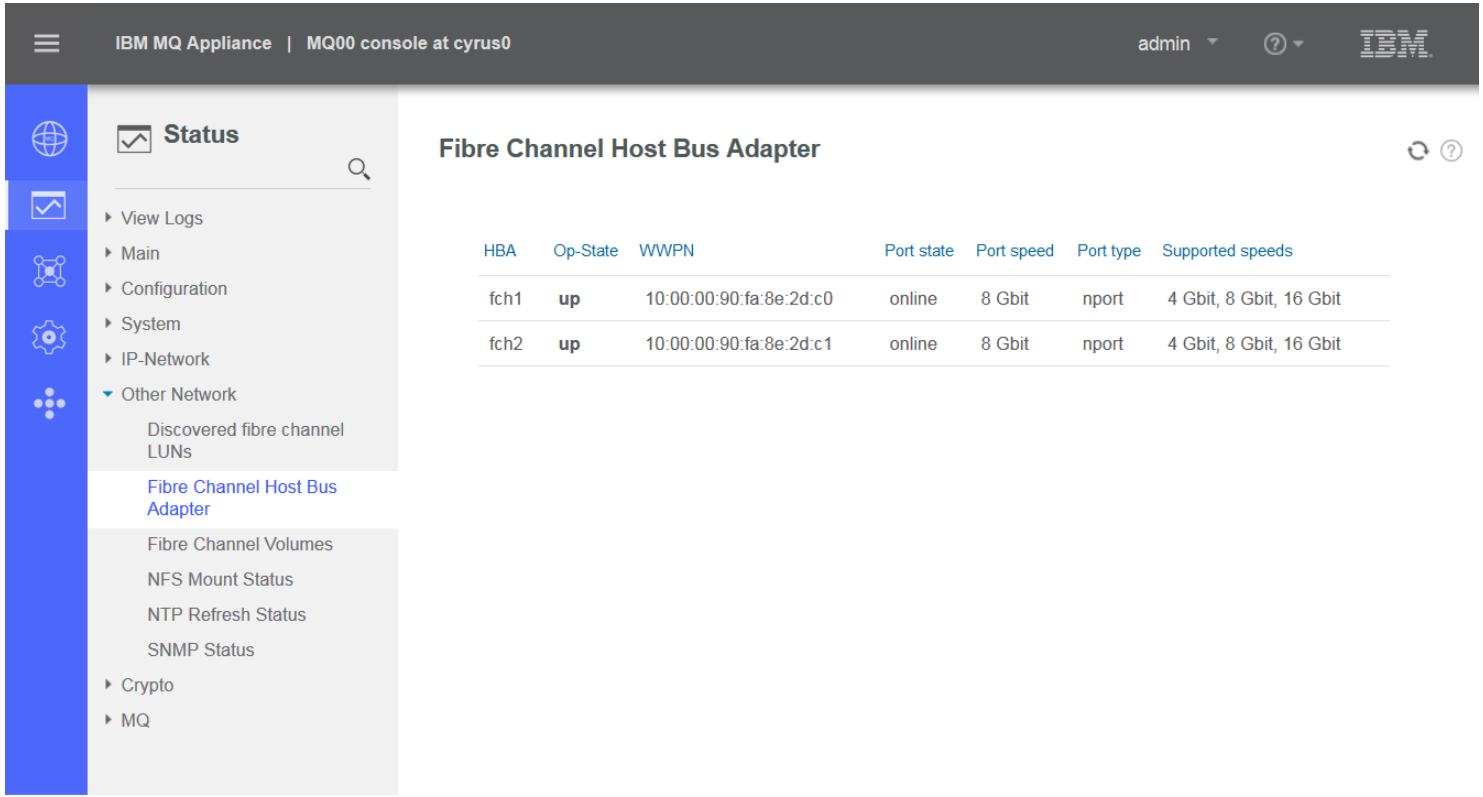
- Not equivalent to full end-to-end signing/encryption using client-side certificates or full disk encryption
  - All clients connecting over a channel share the same certificate
  - The certificates are stored on the same disk as the queue manager data files and are available to MQ administrators or anyone with access to the physical disks
  - We’re looking at improvements we can make to alleviate this vulnerability

SAN support (9.0.4)

- Supports use of external SAN storage for queue manager data
  - Exploits Fibre Channel adapters in the M2000 and M2001
- Requested by customers with high storage or I/O performance requirements, or who employ a SAN solution for disaster recovery
- Two-phase implementation:
  - Phase 1: Standalone queue managers only (not HA)
  - Phase 2: Support for HA queue managers
- Configure the appliance to use SAN
  - Specify a queue manager uses SAN storage when you create it
  - Each queue manager uses a separate SAN partition (disk/volume)

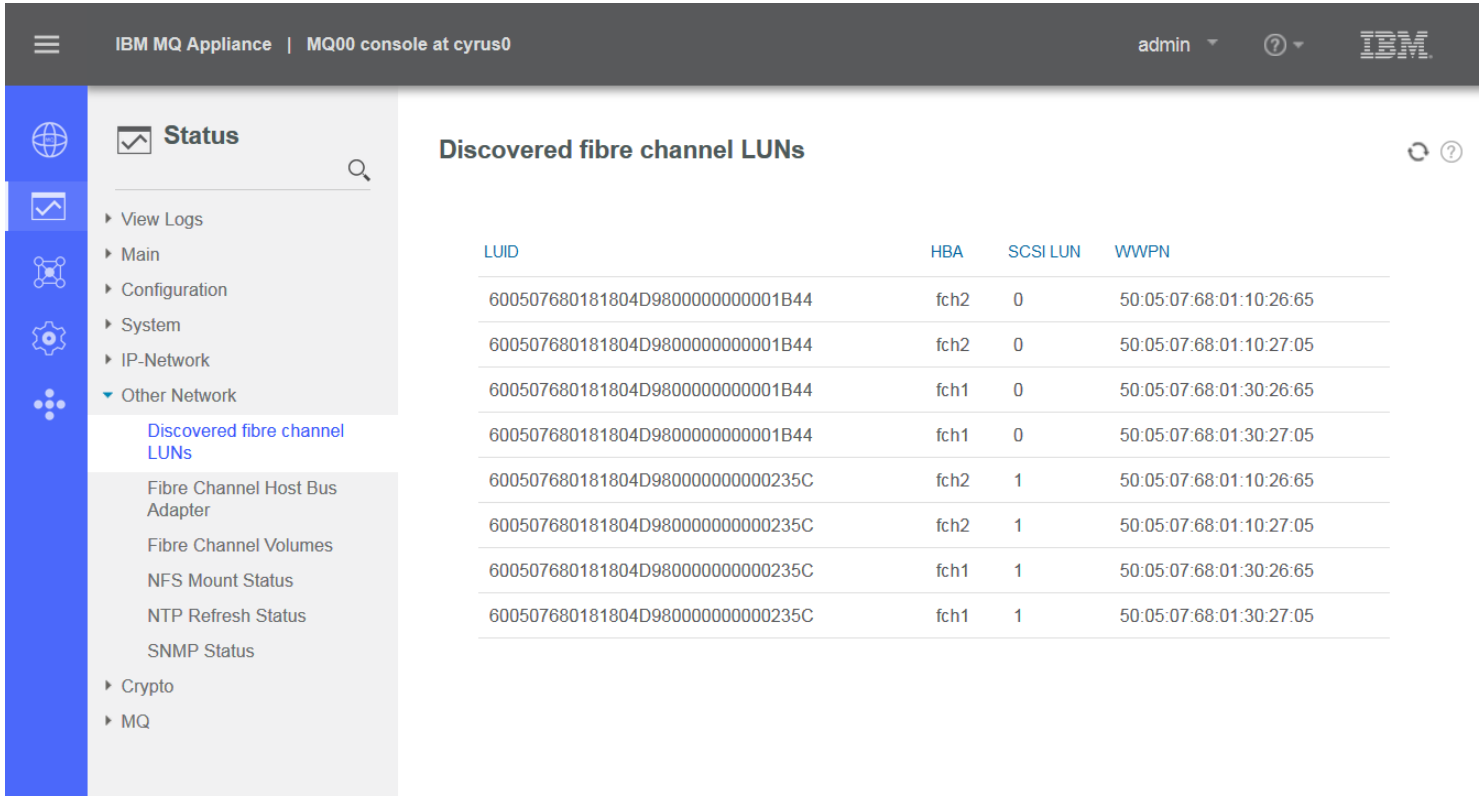
SAN support (9.0.4) - New SAN queue manager

Step 1: Connect to a switched SAN fabric using the fibre channel host bus adapters



SAN support (9.0.4) - New SAN queue manager

Step 2: Configure a LUN for each queue manager in the SAN



LUID	HBA	SCSI LUN	WWPN
600507680181804D9800000000001B44	fch2	0	50:05:07:68:01:10:26:65
600507680181804D9800000000001B44	fch2	0	50:05:07:68:01:10:27:05
600507680181804D9800000000001B44	fch1	0	50:05:07:68:01:30:26:65
600507680181804D9800000000001B44	fch1	0	50:05:07:68:01:30:27:05
600507680181804D980000000000235C	fch2	1	50:05:07:68:01:10:26:65
600507680181804D980000000000235C	fch2	1	50:05:07:68:01:10:27:05
600507680181804D980000000000235C	fch1	1	50:05:07:68:01:30:26:65
600507680181804D980000000000235C	fch1	1	50:05:07:68:01:30:27:05

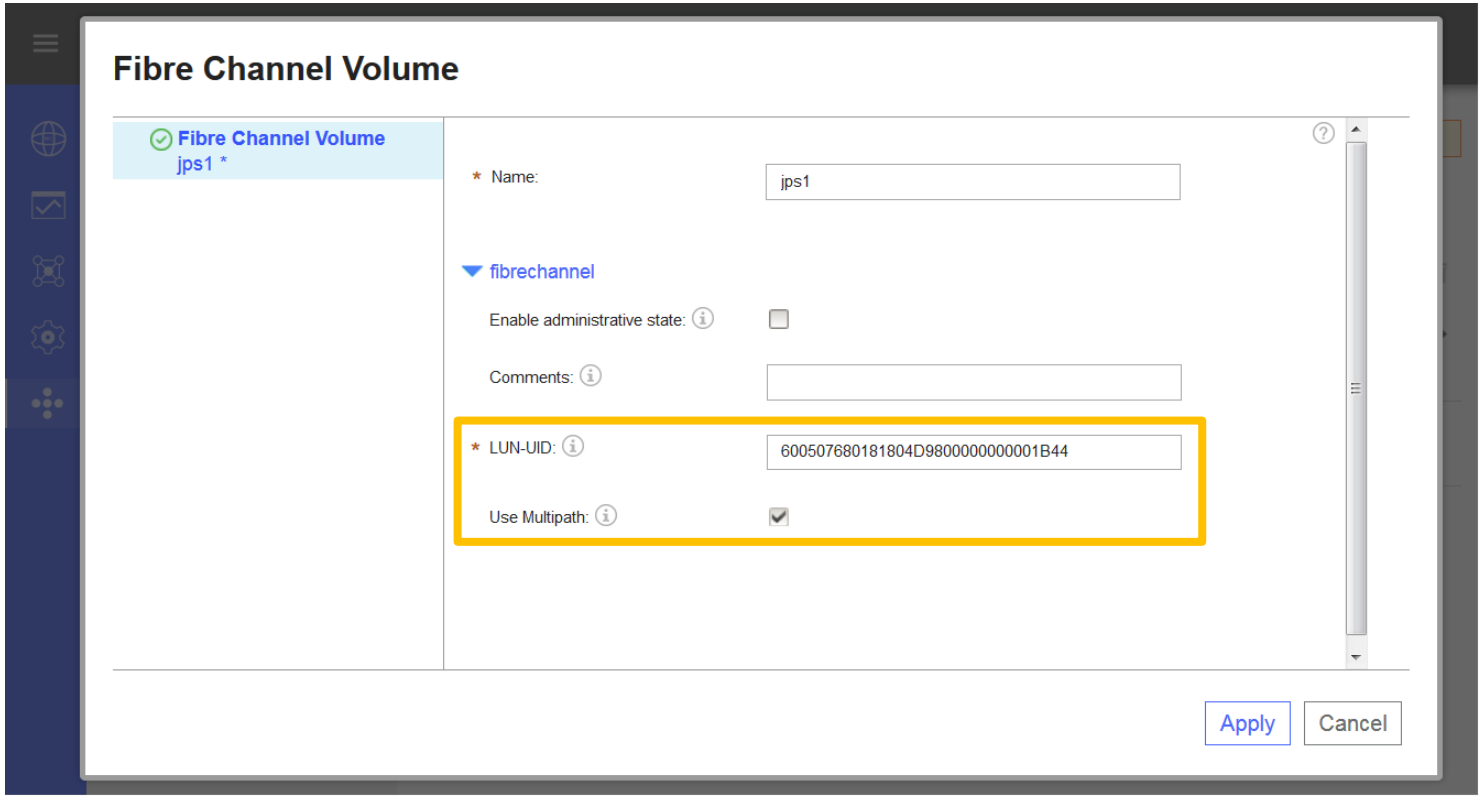
One line shown per LUN for each HBA and WWPN

WWPN = worldwide port number (IP address)

SAN support (9.0.4) - New SAN queue manager

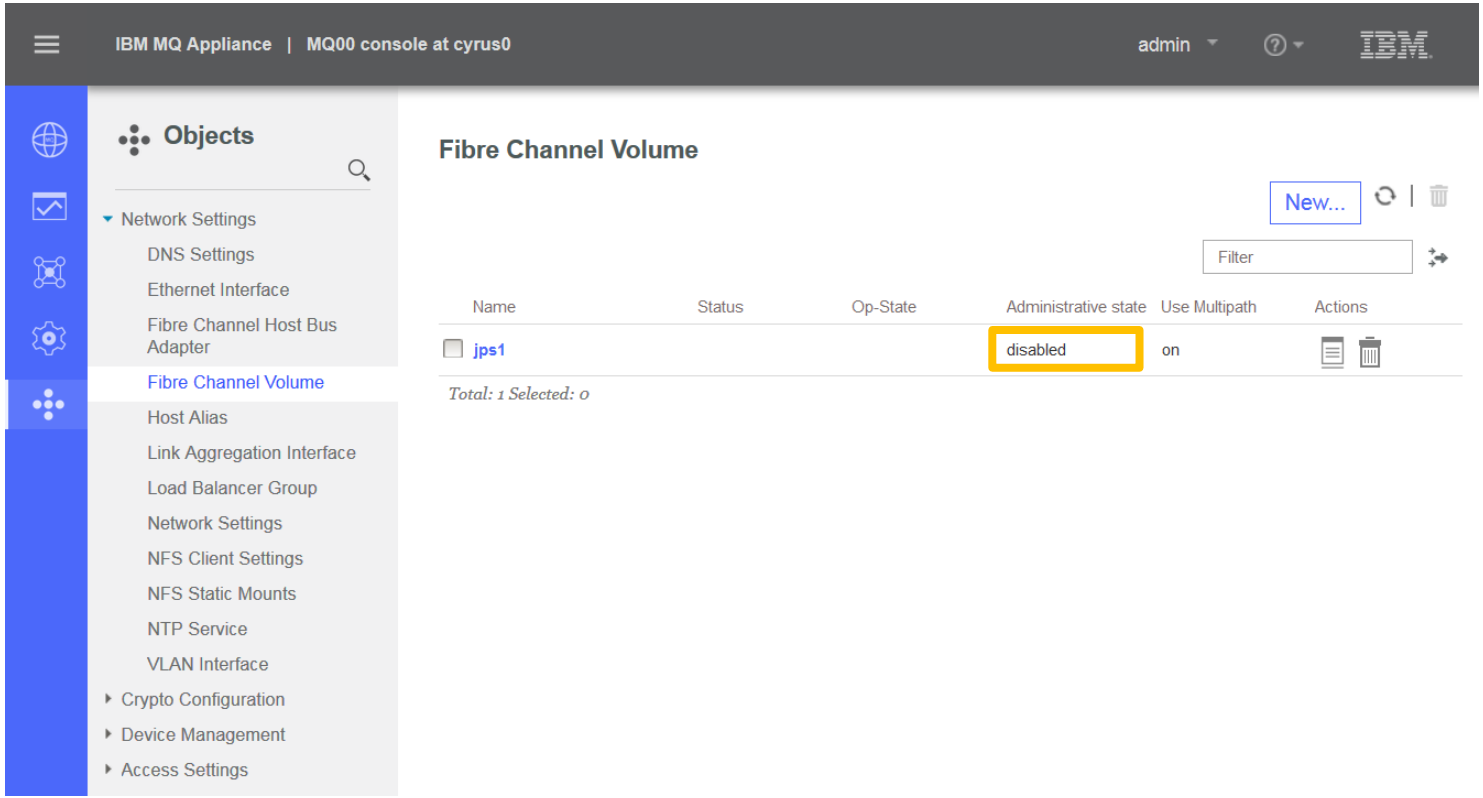
Step 3: Define a fibre channel volume for each LUN

Specify the LUN UUID (WWID) and whether to use multipath



SAN support (9.0.4) - New SAN queue manager

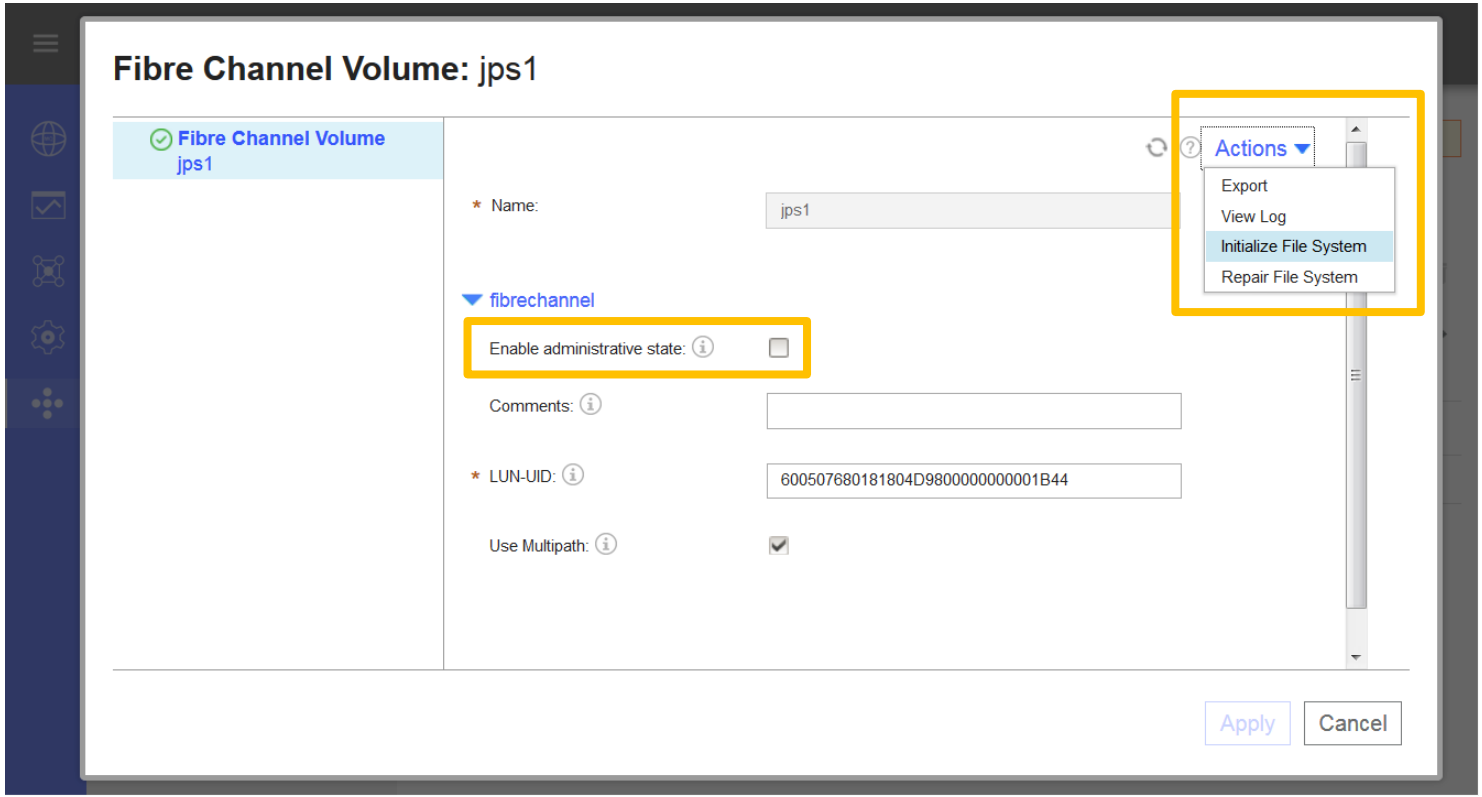
Step 4: Disable the SAN volume (if enabled)



SAN support (9.0.4) - New SAN queue manager

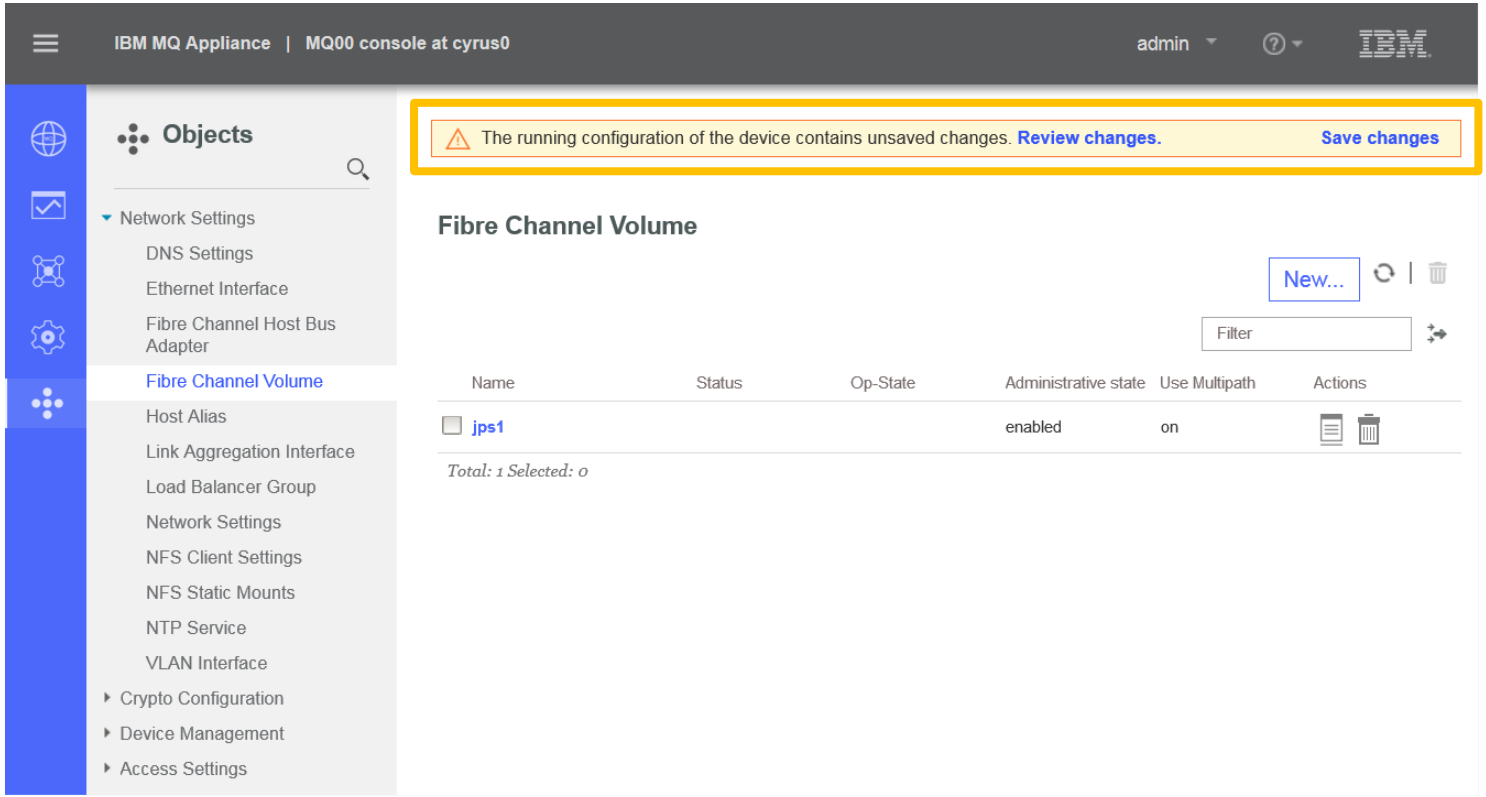
Step 5: Initialize the file system on the SAN volume

… then enable the volume



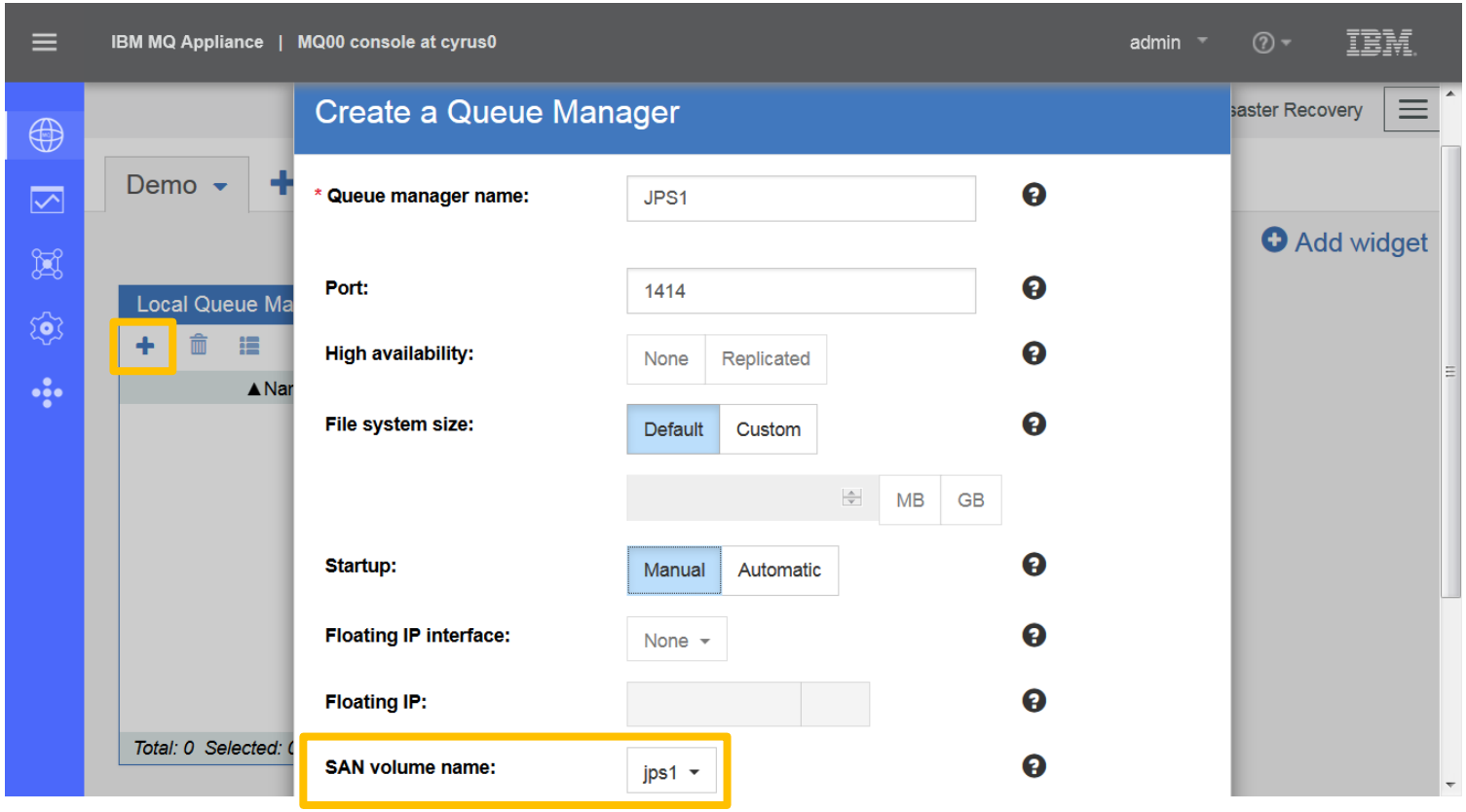
SAN support (9.0.4) - New SAN queue manager

Step 6:
Save the configuration changes



SAN support (9.0.4) - New SAN queue manager

Step 7: Create the queue manager



SAN support (9.0.4) - dspmq

- **dspmq** reports the SAN volume for each queue manager
  - Blank volume name identifies queue managers using local RAID storage

```
mqa(mqcli)# dspmq -o fs
QMNAME(JPS1)                                              FCVOLUME(jps1)
QMNAME(JPS2)                                              FCVOLUME(jps2)
QMNAME(JPS3)                                              FCVOLUME()
```

SAN support (9.0.4) – Managed failover

- Managed fail over of a SAN queue manager to another appliance…
  - On the old appliance:
    - End the queue manager then disable the Fibre Channel Volume object
    - Remove the queue manager definition using **rmvmqinf**

```
mqa(mqcli)# rmvmqinf JPS2
IBM MQ Appliance configuration information removed.
```

  - On the new appliance:
    - Verify SAN connectivity, then define and enable the Fibre Channel Volume object
    - Add the queue manager using **addmqm** in the MQ CLI

```
mqa(mqcli)# addmqm -m JPS2 -fc jps2
IBM MQ Appliance queue manager 'JPS2' added.
```

    - … or select **Recreate SAN queue manager** in the create queue manager UI dialog

SAN support (9.0.4) – Unplanned failover

- Similar to planned failover – assume old appliance is unavailable:
- On the new appliance:
  - Verify SAN connectivity
  - Define and disable the Fibre Channel Volume object
  - Repair the filesystem to clear locks (SCSI persistent reservations)

```
mqa(mqcli)# fibre-channel-fs-repair -f jps2
```

  - Enable the Fibre Channel Volume
  - Add the queue manager using **addmqm** in the MQ CLI

```
mqa(mqcli)# addmqm -m JPS2 -fc jps2
IBM MQ Appliance queue manager 'JPS2' added.
```

    - … or select **Recreate SAN queue manager** in the create queue manager UI dialog

Note: we might change how the locks are cleared before 9.0.4 GA

Resizing queue managers (904)

- For local queue managers only, this can now be modified using new command setmqsize

```
mqa(mqcli)# help setmqsize
Usage: setmqsize -m <qmname> -s <size>

 -m   Queue manager name.
 -s   New file system size.
      Optional size modifiers that can be appended are:
        m - megabytes
        g - gigabytes (default)
```

- HA/DR queue managers must be ‘demoted’ to resize, then returned to HA/DR configuration

Futures

- Candidates for upcoming deliverables:
  - Managed linear logging
  - Support for migrating existing queue managers to a SAN configuration
  - Provision of a secure storage option for queue manager key repositories
  - Integrating MQ error log messages with the system log
  - HA status alerts/events/notifications

- Please let us know which of these candidate items are of interest to you to help us prioritise them (or other items that are not listed)

More information

- IBM MQ Appliance Knowledge Center:
  - https://www.ibm.com/support/knowledgecenter/en/SS5K6E
- MQdev blogs for the appliance
  - https://www.ibm.com/developerworks/community/blogs/messaging?tags=appliance&lang=en
- MPA1: MQ Appliance performance report
  - http://www.ibm.com/support/docview.wss?uid=swg24040125
- MPA2: MQ Appliance HA/DR performance report
  - http://www.ibm.com/support/docview.wss?uid=swg24041474

Questions?