Media Flow Controller 12.3.8 Release Notes

February 2015
Revision 3

Contents

Overview . . . 3
Product Name Changes . . . 3
Media Flow Controller License Is No Longer Required . . . 3
End-of-Life Notification for VXA2010 Series Content Engine . . . 3
Media Flow Publisher End-of-Life Notification . . . 3
Adobe Flash Media Interactive Server End-of-Life Notification . . . 4
Media Flow End-of-Life Policy . . . 4
New and Changed Features in Media Flow Controller 12.3.8 . . . 4
- Enhancement to Content Ingest Manager . . . 4
- Transparent Proxy—DPI Filtering . . . 5
- URL Filtering . . . 5
- CloudFront API . . . 5
- Scheduling Jobs . . . 5

Media Flow Controller Hardware Support and Specifications . . . 5
Upgrading Media Flow Controller to Release 12.3.8 . . . 6
Resolved Issues in Media Flow Controller Release 12.3.8 . . . 6
Limitations in Media Flow Controller Release 12.3.8 . . . 7
Outstanding Issues in Media Flow Controller Release 12.3.8 . . . 11
- Disk Subsystem . . . 11
- General Caching System . . . 14
- Installation . . . 15
- Management and Logging . . . 18
- Network Subsystem . . . 29
- Reverse Proxy . . . 29
- Transparent and Reverse Proxy . . . 33
- Transparent Proxy . . . 33

Documentation Updates . . . 34
New CLI Commands Introduced in Media Flow Controller Release 12.3.8 . . . 34
Requesting Technical Support . . . 36
- Self-Help Online Tools and Resources . . . 36
- Opening a Case with JTAC . . . 36

Revision History 37

Overview

These release notes provide the latest information about Media Flow Controller Release 12.3.8.

The *Media Flow Controller 12.3.8 Release Notes* accompany the *Media Flow Controller 12.3.x Installation Guide*, *Media Flow Controller 12.3.8 Administrator's Guide*, and the *Media Flow Controller 12.3.8 CLI Command Reference*.

Product Name Changes

As of October 2, 2012, the Media Flow product names changed to Junos Content names and are reflected as such on the Juniper Networks Web site. However, the current product software and documentation still use the Media Flow product names.

Old Media Flow Names	New Junos Content Names
Media Flow Controller	Junos Content Encore
Media Flow Activate	Junos Space Content Director
VXA Series Media Flow Engines	VXA Series Content Engines

Media Flow Controller License Is No Longer Required

You are no longer required to install the Media Flow Controller license, LK2-MFD. You are also no longer required to install the restricted license, LK2-RESTRICTED_CMDS, for full shell, device, and CLI access to the Media Flow Controller software. The only license that you are now required to install is the SSL license, LK2-SSL, for SSL service. The installed Media Flow Controller license displays as **unrecognized** if you use the **show license** CLI command, and **unknown** if you upgrade with that license already installed. The Media Flow Controller Web interface no longer displays the license status in the top right corner, but does display the status if the license is expired or corrupted.

End-of-Life Notification for VXA2010 Series Content Engine

Juniper Networks is ending the life of the VXA2010 Series Content Engine on May 1, 2013. The replacement device is the VXA2002 Series Content Engine. However, for the VXA2010 Series Content Engine, there is no impact to software support. See JTAC Technical Bulletin PSN-2013-05-936 at http://kb.juniper.net/InfoCenter/index?page=content&id=TSB15977&actp=search&viewlocale=en_US&searchid=1374868037262. For questions, contact Juniper Networks Customer Service.

Media Flow Publisher End-of-Life Notification

Juniper Networks is ending the life of the software product Media Flow Publisher (EOL model number S-JMFPUB-RTU) as of Media Flow Controller Release 12.2.5, May 1, 2013. Media Flow Publisher, a Media Flow Controller application, provided online and offline

video preparation for delivery to various adaptive bit rate players, such as Microsoft Silverlight Smooth Streaming, Apple HTTP Live Streaming, and Adobe HTTP Dynamic Streaming used in mobile, desktop, and TV devices. Therefore, Media Flow Publisher is no longer supported and cannot be ordered. See JTAC Technical Bulletin PSN-2013-05-936 at http://kb.juniper.net/InfoCenter/index?page=content&id=TSB15977&actp=search&viewlocale=en_US&searchid=1374868037262. For questions, contact Juniper Networks Customer Service.

Adobe Flash Media Interactive Server End-of-Life Notification

Juniper Networks is ending the life of the software product FMIS License with MFC Cache Connector S-JMFFMS-SW as of October 1, 2012. See Product Support Notification, PSN-2012-09-729 at https://www.juniper.net/alerts/viewalert.jsp?actionBtn=Search&txtAlertNumber=PSN-2012-09-729&viewMode=view. Therefore in the Media Flow Controller 12.2.3 release, the Adobe® Flash® Media Interactive Server license to stream Flash videos over the Real-Time Messaging Protocol (RTMP) is no longer supported and cannot be ordered. Media Flow Controller had supported Adobe FMS 3.5 or FMS 4.0. For questions, contact Juniper Networks Customer Service.

Media Flow End-of-Life Policy

Software releases are supported for up to 18 months or 2 subsequent releases, whichever occurs first. At that point, the software reaches its end of engineering (EOE) date and is no longer actively supported by Engineering. Update releases (for example service, maintenance, or patch) will no longer be created for major software releases that have reached the EOE milestone. All software releases are supported by JTAC on a limited basis for up to an additional 12 months or 2 subsequent releases, whichever occurs first. At that point, the software reaches its end-of-life and end-of-support (EOL/EOS) date.

New and Changed Features in Media Flow Controller 12.3.8

Media Flow Controller Release 12.3.8 includes these new features and enhancements to existing features.

- Enhancement to Content Ingest Manager on page 4
- Transparent Proxy—DPI Filtering on page 5
- URL Filtering on page 5
- CloudFront API on page 5
- Scheduling Jobs on page 5

Enhancement to Content Ingest Manager

Prior to Release 12.3.8, the Content Ingest Manager allows users to fetch files from the same domain as the base URL by default. Starting with Release 12.3.8, the Content Ingest Manager allows users to fetch files across domains referenced from the same base URL. For relative URLs, Media Flow Controller uses the domain of the base URL. For absolute URLs, Media Flow Controller uses the domain specified in the absolute URL. To enable cross-domain fetches, use the **crawler *name* action x-domain crawl** command. To disable this feature, use the **crawler *name* no action x-domain crawl** command.

Transparent Proxy—DPI Filtering

Filtering policies based on Deep Packet Inspection (DPI) can help improve caching for transparent proxy. Media Flow Controller has tools (DPI tool and log analyzer tool) to process HTTP packets in traffic mirrored from MX Series routers and to create a firewall filter policy. The DPI tool processes the HTTP packets and generates a log file that is processed by the log analyzer to determine whether the URI is cacheable by matching domains specified in the configuration file. If the domain matches, the log analyzer creates a firewall filter policy that is applied to the router or written to a file depending on the log analyzer tool configuration.

URL Filtering

URL filtering is used to allow or deny access to HTTP content based on the hostname and the absolute path of the URL. It can be implemented with an HTTP proxy (proxy mode) or with a DPI mechanism (packet mode). Proxy mode handles symmetric traffic configurations where the input and output traffic pass through the proxy. Packet mode handles asymmetric traffic configurations where the input traffic passes through the DPI node.

CloudFront API

Media Flow Controller Release 12.3.8 includes this feature that is not fully qualified.

Amazon CloudFront is an Amazon Web Services (AWS) content delivery service. The Amazon CloudFront API is a REST API that can be used to configure virtual Junos Content Encore instances.

Documentation for this feature is included in this release, but this feature is not supported in Release 12.3.8.

Scheduling Jobs

Media Flow Controller Release 12.3.8 includes this feature that is not fully qualified.

To support the job scheduler, use these CLI commands to enable this feature:

- **jobs ***—Configure job schedules.
- **no jobs**—Disable job scheduler configuration.
- **show jobs ***—Display configured job schedules.

Media Flow Controller Hardware Support and Specifications

The Media Flow Controller software supports all platforms in the following product series. For the latest hardware support and specifications, see the *Media Flow Controller* product datasheet on the Juniper Networks website http://www.juniper.net/us/en/products-services/content-media/media-flow-controller/.

- VXA Series Content Engines
- Select generic x86-64 servers

Upgrading Media Flow Controller to Release 12.3.8

Use the criteria below to determine how to upgrade to Media Flow Controller 12.3.8:

NOTE: You cannot upgrade directly from Media Flow Controller Release 11.X to 12.3.8. You must first upgrade to Release 12.2 and then upgrade to Release 12.3. If you do not follow this upgrade path, you might have to reinstall the device. An alternative method to first upgrading to Media Flow Controller Release 12.2 is explained in the "Upgrade Order Requirements" section of the *Media Flow Controller 12.3.x Installation Guide*.

- Non-VXA hardware users should use the standard upgrade procedure documented in the *Media Flow Controller 12.3.x Installation Guide* to upgrade to Release 12.3.
- VXA customers upgrading from Media Flow Controller 12.1 or later should use the standard upgrade procedure documented in the *Media Flow Controller 12.3.x Installation Guide* to upgrade to Release 12.3.
- VXA customers upgrading from any version prior to Release 12.1 must follow the procedure below. Customers upgrading from Media Flow Controller prior to Release 11.B.3 must upgrade to Media Flow Controller 11.B.3 or 11.B.4 before following the procedure in this section.

Resolved Issues in Media Flow Controller Release 12.3.8

- **PR 1060490**
  Symptom:
  Releases prior to Release 12.3.8-5 are susceptible to CVE-2015-0235, the buffer overflow bug that affects the **gethostbyname** and **gethostbyname2** function calls in the **glibc** library. This vulnerability allows remote attackers, who can make application calls to either of these functions, to execute arbitrary code with the permissions of the user running the application. The patch for CVE-2015-0235 addresses this vulnerability and is available in Release 12.3.8-5 or later.
- **PR 1056923**
  Symptom:
  When Media Flow Controller is deployed in a clustered topology and origin selection is made using a cluster-hash server map, the delivery service can be restarted under heavy load. This issue affects only this specific configuration and not generic proxy deployments where origin selection is made using FQDN or is based on the DNS resolution of HOST header. This issue is resolved in Release 12.3.8 or later.
- **PR 1034405**
  Symptom:
  Releases prior to Release 12.3.8-4 are susceptible to the SSLv3 vulnerability known as Padding Oracle On Downgraded Legacy Encryption (POODLE). The vulnerability makes it easier for man-in-the-middle attackers to decrypt messages using the way SSLv3

handles padding bytes. The patch for CVE-2014-3566 addresses this vulnerability and is available in Release 12.3.8-4 or later.

- **PR 1031100**
  Symptom:
  The Bash shell used in releases prior to Release 12.3.8-2 is susceptible to the ShellShock vulnerability. The vulnerability is not exposed in the data path, but it can be exploited by someone with access to the Media Flow Controller Web interface. The patches for CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187 completely remove the ShellShock vulnerability. These patches are available in Release 12.3.8-3 or later.
- **PR 1025940**
  Symptom:
  Eviction might stop when the namespace is deleted on a busy system during the eviction process. When the namespace corresponding to the object currently being deleted is removed during the eviction process, then the eviction process might get stuck and block further evictions. This issue is resolved in Release 12.3.8 or later.
  Workaround:
  If eviction on a system stops due to this issue, use the **service restart mod-delivery** command to restart the delivery service and restore the system to its normal state.
- **PR 991515**
  Symptom:
  When caching Netflix video content, the client player would sometimes freeze and stop playing the video. This issue is resolved in Release 12.3.8.

Limitations in Media Flow Controller Release 12.3.8

The following is a list of limitations of Media Flow Controller Release 12.3.8.

Management and Logging

- **PR 764895**
  Symptom:
  The CLI command **configuration revert factory keep-connect** does not preserve the bond or port aggregation configuration. The factory reset **keep-connect** preserves the configuration necessary for network connectivity (interfaces, routes, and ARP). However, it does not preserve the bond configuration.
  Workaround:
  Copy the bond configuration before factory reset, and restore it after the factory reset.
- **PR 764934**
  Symptom:
  For X-Accel-Cache-Control, the attribute update does not occur during revalidation in a disk with the cache-age set to the default value (0 seconds).
- **PR 765951**
  Symptom:
  The response time when serving objects from disks is higher during eviction. Eviction of content from the disk cache results in a delete operation. Fetching of content from disk cache results in a read operation. While Media Flow Controller delivers data from disks during eviction of URIs, the delete operation and read operation occurs

simultaneously. The response time for an object fetch request has been observed to be higher in this scenario.

- PR 766244
  Symptom:
  Media Flow Controller supports HTTPS authentication, but encryption is not supported. Even though encryption is not supported, online help and the **show virtual-host list** command indicate that cipher suites can be configured on the Media Flow Controller. The unsupported DSA ciphers are listed in cipher help context. Even though DSA ciphers are not supported in this release, the ciphers are still listed in cipher help context.

- PR 766363 and PR 766392
  Symptom:
  Header manipulation actions, applied by the Policy Engine **pe_http_send_response** and **pe_om_send_request** processes, do not consider the headers inserted by a namespace. A configuration option exists at the **namespace** CLI level to add or delete headers towards the client response and to add headers towards the origin request. If you configure header manipulation actions at both **namespace** CLI and Policy Engine levels, the header manipulation actions applied at the Policy Engine level do not consider the headers manipulated by the **namespace** CLI level before taking the action.

- PR 766528
  Symptom:
  When you configure **delivery protocol http client-request cache-hit action revalidate-always** from the configuration mode, the CLI returns an internal error. Media Flow Controller provides an option to set the **cache-revalidate** option for a namespace that does transparent proxy caching. Before setting the **cache-revalidate** option, the CLI checks whether the namespace is configured for reverse proxy or for transparent proxy caching. When you issue this **cache-revalidate** CLI command before configuring the namespace for transparent proxy caching, the CLI displays the following error message: "% An internal error occurred."
  Workaround:
  Configure the namespace origin-server option before issuing **cache-revalidate**.

- PR 766700
  Symptom:
  Media Flow Controller cannot stop or abort a pre-fetch job if the URLs listed are currently being processed or downloaded.

- PR 766798
  Symptom:
  When the neighbor ARP table overflows, Media Flow Controller cannot connect to the origin server.

  When running the transparent proxy system test using more than 16,000 unique client IP addresses and origin server IP addresses running in the same IP subnet as the Media Flow Controller, the neighbor ARP table quickly overflows. This ARP table overflow results in a "Connection" failure when Media Flow Controller attempts to connect to the origin server. This in turn results in a syslog "Network thread stuck" message as one of the network threads utilizes 100 percent of the CPU.
  Workaround:

Increase the number of ARP entries using the **delivery protocol http conn-pool max-arp-entry *number*** command to configure up to 16,000 entries. In most production deployments, the Media Flow Controller will not have 16,000 directly attached clients. On the same subnet there will be a router between the Media Flow Controller and the clients.

- PR 766840
  Symptom:
  When aggressive cache-fill is configured in Media Flow Controller, the "Last 24 Hr" field in the dashboard "Cache Hit Ratio" shows a negative value. This occurs when the client requests partial data, and Media Flow Controller downloads the full file from origin server. This might lead to the scenario where more data is downloaded from the origin and less data is served to the client.

- PR 766909
  Symptom:
  When the bandwidth available under a namespace is oversubscribed, the client sees an increased latency in data delivery.

  The resource pool imposes two limits on the client sessions: the client session limit and client delivery bandwidth limit. Both of these limits are applied at the resource pool level. When the number of sessions on the resource pool exceeds the configured limit, then the additional clients are not allowed to access the resource pool. In the case of a bandwidth limit, if N clients are able to pull data occupying the whole bandwidth pipe reserved for the resource pool and if more client connections pass through the resource pool, the existing N clients see a latency increase in data delivery.

  This is expected behavior. As new connections come in to an already saturated resource pool, all collections share a limited bandwidth and experience latency and lower throughput than they did before the resource pool was fully consumed.

- PR 766970
  Symptom:
  The connect-timeout value has no impact on the watchdog heartbeat request, and the Media Flow Controller is marked as down before reaching the connect-timeout value.

  The connect-timeout value is actually MIN (read_timeout, connect_timeout). If the read-timeout value is 100 milliseconds and the connect-timeout value is 10 seconds for a heartbeat, then the actual connect-timeout value is taken as 100 milliseconds.

- PR 767003
  Symptom:
  The command **delivery protocol http listen port 8080** is accepted in the CLI configuration. However, the command does not work (that is, the delivery engine does not listen on port 8080) and the system does not report any error. Port 8080 is used by the internal Web server that serves administrative Web GUI pages.
  Workaround:
  If you need to configure port 8080 for the delivery engine to listen, first configure port 8081 for the internal Web server using the command **web http port 8081**.

- PR 767063
  Symptom:

The access log records "%s" (HTTP status) field has a value of 0 for HTTP/0.9 responses. Media Flow Controller supports HTTP/0.9 requests after Release 11.B.2 and tunnels such requests. For HTTP/0.9 requests, the responses do not have any HTTP headers, so the "%s" field in the access log has a value of 0.

- **PR 767285**
  Symptom:
  Newly ingested objects are picked up for eviction even though there are other objects in the cache that are relatively cold and have not been accessed recently.

  When the eviction process starts, the hotness of all the objects is recalculated through a decay mechanism to ensure that the system-wide hotness of all the objects is normalized. This decay process would normally reduce the hotness gradually. However, in this case, if some objects are hot even after the decay, they would still be hotter than the new objects that are being added. As a result, new objects are evicted when compared to the ones that are not being frequently accessed.

- **PR 767332**
  Symptom:
  When many parallel connections hit the objects in the disk, excess connections are tunneled after a certain threshold so that user sessions avoid suffering abnormal latencies.

- **PR 767381**
  Symptom:
  Pinned objects are deleted.

  If the metadata partition of a disk is filled to capacity, an eviction mechanism is initiated to free up the metadata partition space. This eviction deletes objects even if they are pinned. This metadata eviction is applicable only to SSD drives.

- **PR 767603**
  Symptom:
  Resource pool configuration allows you to configure the session limit up to the maximum concurrent sessions configured at the network level.

  Specify the maximum number of concurrent sessions that the Media Flow Controller can accept using the **network connection concurrent session** CLI command (which is a maximum of 256,000 for this release). This value can be divided across different resource pools and configured as the session limit. Although the configuration is limited by the connections, the resource pool sessions are accounted for at the namespace level (only for active data transferring sessions). Media Flow Controller can support up to 256,000 connections, from which 64,000 connections can be active. If you assign more than a 64,000 connection session limit to one of the resource pools, the particular resource pool can use the full system capacity of 64.000 active sessions and degrade performance of other resource pools.
  Workaround:
  Although the system allows you to configure resource-pool session limits based on the maximum number that can be open, you can configure the session limits based on maximum number of active sessions expected through the resource-pool.

- **PR 767634**
  Symptom:

Even when it is not bound to a namespace, the resource pool availability field in the native application section shows the result as “true.”
Workaround:
None. The resource pool availability is tied to whether or not the resource pool is present in the system and does not represent its binding to one or more namespaces.

- **PR 767765**
  Symptom:
  Load feedback API does not support connection persistence, and hence you cannot use a single connection to send multiple HTTP GET requests. For every request, the load feedback service responds with a “Connection: Close” HTTP header, which instructs the client to close the connection.

- **PR 767768**
  Symptom:
  When Media Flow Controller is configured in aggressive mode and the client sends a time-based seek request, it forwards the actual request to the origin. In addition, it sends one more request to fetch an object. This is expected behavior because the purpose of aggressive mode is to cache the entire object, regardless of the client request. Thus, the Media Flow Controller is behaving as expected.

- **PR 763177**
  Symptom:
  Media Flow Controller has the option of adding policies at the client and origin sides of a data connection. If a user connection hits a namespace that is configured to serve data from an origin server that is connected to Media Flow Controller through the NFS protocol, then the origin side policies applied in the system will not have an impact on the data connection.

Outstanding Issues in Media Flow Controller Release 12.3.8

The following is a list of outstanding issues in Media Flow Controller Release 12.3.8.

Disk Subsystem

- **PR 765890**
  Symptom:
  Ingestion is slower if directories have a large number of objects.

  Workaround:
  We recommend that you spread the objects across multiple directories.

- **PR 766251 and 766284**
  Symptom:
  In rare cases, when Media Flow Controller is under load, it is not possible to inactivate and disable cache disks using the following commands: **media-cache disk *disk name* cache (enable | disable)** and **media-cache *disk name* status (active | inactive)**. If you execute these commands while running traffic, a drop in delivery throughput might occur. Sometimes the command itself might not be successful or might result in the delivery engine service restart.
  Workaround:
  Use disk management CLI commands during maintenance window when traffic is low.

- PR 766308
  Symptom:
  The **Discarding eviction for /nkn/tmp/dm2_disk_evict.1.dc_<N>** error message is seen often in the system log. This message indicates that eviction is starting, which is a normal process in the Media Flow Controller. This message does not indicate a real error condition, and you can ignore it.

- PR 766426
  Symptom:
  When a disk is deactivated, cache latency might increase. In one particular lab test, transactions per second (TPS) dropped from 1000 to 700.
  Workaround:
  Perform disk activation and deactivation during a maintenance window when TPS is at its lowest.

- PR 767117
  Symptom:
  If multiple disks are enabled simultaneously using the **media-cache disk dc_x cache enable** CLI command, the pre-reading of the objects in the enabled disks completes prematurely without fully reading all the entries.

  When a disk is enabled, metadata for all objects in the disk is read into the dictionary. However, if multiple disks are enabled at the same time (for example, by using a script or typing the CLI commands in sequence one after another), some of the metadata in some disks is not read. This could cause already available objects to be re-ingested and result in unnecessarily wasting disk space. This issue does not occur when Media Flow Controller is restarted with all the disks enabled.
  Workaround:
  Restart Media Flow Controller with all disks enabled, or enable the disks one-by-one after validating that the pre-read process for the enabled disk has completed.

- PR 767147
  Symptom:
  Response time increases when the system pre-reads metadata information from the disks. When the delivery service in Media Flow Controller is started, it pre-reads the metadata information from the disks once and places it into RAM to avoid costly disk lookup time when the data is later requested by the client. During this period, you might see an increase in response time.
  Workaround:
  Wait until the pre-read is complete before putting the Media Flow Controller in service.

- PR 767473
  Symptom:
  Persistent configured disks are listed as “dc_” instead of “ps_.” The CLI command **persistent-store disk list** used to list the configured persistent store disks shows the device listed as “dc_.” The device should be used with the name “ps_1” when configuring delivery from this disk.

  

  NOTE: Only a single persistent device is supported for this release.

- **PR 767814**
  Symptom:
  For non-VXA systems that have Smart Array disk controllers, the disk-related statistics in the system section returned by load feedback API are not computed and are always displayed as zero (0).

- **PR 768135**
  Symptom:
  Disabling a cache takes more time and appears to hang if the data set has a large number of files per container. If the data set that is cached has a large number of files per container (directory) and traffic is being served for that profile, a cache disable command waits and appears to hang. The CLI command times out without reporting any status.

- **PR 768307**
  Symptom:
  With the root disk enabled for caching, the disk dc_0 is not listed in media-cache listing. By default, the root disk is not enabled for caching. If the root disk is enabled for caching, Media Flow Controller treats the cache as dc_0.

- **PR 768371**
  Symptom:
  On the VXA2000 Series Content Engine, the disk list is not always sorted. This can occur when hot-plugging to an empty slot and is sometimes seen after a clean manufacture.

- **PR 773661**
  Symptom:
  When changing the SAS disk block size from 256 KB (which was done earlier) back to 2 MB by reformatting it, reformatting does not occur properly without a delivery service restart. If you do not restart the delivery service, premature eviction occurs.

- **PR 775737**
  Symptom:
  Any bad disk can overuse system resources and degrade the data delivery of the other disks as well. One bad disk in a VXA Series Content Engine can degrade the data throughput from 100 percent to 70 percent.
  Workaround:
  If there is a degrade in the data throughput, check for bad disks and replace them.

- **PR 801637**
  Symptom:
  Sometimes when Media Flow Controller comes online after a reboot, the disks might not get changed to the "cache running" state and are stuck in the "conversion of disk cache version failed" state, which can be viewed using the **show media-cache disk list** CLI command.
  Workaround:
  This is a temporary state that you can recover from by using the following CLI commands:
  pm process nknexecd restart
  service restart mod-delivery

- **PR 807353**
  Symptom:
  The cache pinning feature works on objects that are ingested to the lowest disk tier. However, cache pinning does not work for objects promoted due to hotness or highest object-size using the **delivery protocol http origin-fetch content-store media cache-tier highest object-size** CLI command. If you configure this CLI command and if an object enters directly into the SSD, the object is not pinned.
- **PR 838382**
  Symptom:
  On a VXA2000, if Root disk mirroring option is enabled, a new disk may not be detected if it is hot plugged.
  Workaround:
  After plugging in a new disk, reboot the box and the disk will be detected on booting

General Caching System

- **PR 764608**
  Symptom:
  In rare conditions, when the core cache engine service crashes, no snapshot is generated and the system CPU reaches 100 percent.
- **PR 765178**
  Symptom:
  When Media Flow Controller caches a partial object, an origin server changes cache-control headers for that same object and a client requests the remainder of the object, the Media Flow Controller closes the client connection and does not serve the object.
  Workaround:
  Request the object from the client to Media Flow Controller with **Cache-control: max-age=0**. This action deletes the partial content from Media Flow Controller cache and further requests are handled properly.
- **PR 766559**
  Symptom:
  The **delivery protocol http req-length maximum** CLI command, that configures the maximum request header size, does not work for values greater than 8 KB. Requests of a size greater than 8 KB are tunneled to origin, and responses to such requests are not cached.
- **PR 766814**
  Symptom:
  The origin server sees two requests from Media Flow Controller for an asset that does not exist in the origin server when a virtual player is configured:
  - A virtual player is associated to a namespace.
  - A request is received by Media Flow Controller for an asset that is unavailable in either Media Flow Controller or the origin server.
  - Media Flow Controller responds to the client with a 404 code.

However, two requests are sent to the origin server as observed in the origin server access logs.

- **PR 797111**
  Symptom:
  In case of namespaces, such as a server-map based namespace or a transparent proxy namespace, where the objects corresponding to multiple domains get cached, if you want to delete objects matching a pattern from a particular domain, use the **namespace *name* object delete *pattern domain port*** CLI command. However, this command currently deletes all the URIs matching the pattern from all the domains.

Installation

- **PR 765224**
  Symptom:
  Due to the underlying kernel change which brings out lot of positive improvements, the memory usage of the system has been increased. It is recommended that you decrease the RAM cache size by 2 GB, which will release 2 GB memory for use by other system processes. Please note the following recommended memory settings:
  - 128K client connections - pre-12.3.2 images : 16 GB ram-cache
  - 128K client connections - 12.3.2 : 14 GB ram-cache
  - 256K client connections - pre-12.3.2 images : 14 GB ram-cache 256K client connections - 12.3.2 : 12 GB ram-cache

  Please note that the settings for the 128K client connections settings is applicable for current Tproxy deployments.

- **PR 766626**
  Symptom:
  Due to timing issues, there is a case where no disks are made available for caching delivery service. This problem is easily recognized by verifying **show media-cache disk list** output. The command will show no valid disks, indicating that no new objects can be stored to disk and no pre-existing cached objects can be read from disk.
  Workaround:
  Restart the mod-delivery service using the following command: **service restart mod-delivery**.

- **PR 774174**
  Symptom:
  If multiple Application Server Modular Line Cards (AS-MLC) installed on the same router are rebooted simultaneously, the time to boot up all cards might be double the time to boot up one card.

- **PR 777223**
  Symptom:
  If an Application Services Modular Storage Card (AS-MSC) daughter card is inserted while the Application Services Modular Processing Card (AS-MXC) is up and running the Media Flow Controller software, the DIMMS on the AS-MSC card do not start.
  Workaround:

After inserting the AS-MSC daughter card, restart the entire Application Services Modular Line Card (AS-MLC) by turning off and off the FPC slot.

- PR 809429
  Symptom:
  While installing Media Flow Controller software on the VXA2000 Series Media Flow Engine using a CD-ROM or USB, sometimes the CD-ROM and USB might get bypassed and the system might fall back to the existing image in the system. Rebooting the system helps to restore the correct boot sequence. However, this action might not be an issue in normal deployment scenarios as the system is installed with an image when the hardware is shipped initially and you might need to upgrade the image thereafter.
  Workaround:
  Reboot the system to restore it.

- PR 819883
  Symptom:
  If a VXA2000 Series Content Engine is loaded with more than 2 disks, and if you try to install using a DVD or USB, on reboot the system fails to boot from the DVD and falls back to the network boot.
  Workaround:
  Remove all cache disks from the system, leave only the root drive, and install. Then, plug in the cache disks.

- PR 836662
  Symptom:
  Few non-delivery impacting warning messages are printed in the system log when the Media Flow Controller is installed. These messages do not impact the functionality of the delivery module. Ignore the following messages during installation:

  - FATAL: Could not load /lib/modules/2.6.32-220.23.1.el6JUNIPERsmp/modules.dep: No such file or directory
  - udevd-event[724]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.2/host5/ioerr_cnt' failed
    |udevd-event[1719]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1f.2/host1/target1:0:0/ioerr_cnt' failed
    udevd-event[1735]: wait_for_sysfs: waiting for '/sys/devices/pci0000:00/0000:00:1d.7/usb2/2-5/2-5:1.0/host6/target6:0:0/ioerr_cnt' failed
  - Starting ipmi drivers: ipmi_si:
    Unable to find any System Interface(s)[FAILED]
    Could not open device at /dev/ipmi0 or /dev/ipmi/0 or /dev/ipmidev/0:
    No such file or directory
  - Nov 28 07:22:45 vxa12-2 nknlogd:
    TID 1115121984: [unk.ERR]: unk: dbglog_epollin(), log_debuglog.c:39, build 238:
    No such file or directory: recv failed
  - Nov 28 07:12:13 localhost kernel: ACPI Error (dsfield-0143):
    [CAPB] Namespace lookup failure, AE_ALREADY_EXISTS
    Nov 28 07:12:13 localhost kernel: ACPI Error (psparse-0537): Method parse/execution failed [_SB_.PCI0._OSC]

(Node ffff88021f80d820), AE_ALREADY_EXISTS

- PR 839808
  Symptom:
  The Application Services Modular Line Card (AS-MLC) fails to boot up the Media Flow Controller software when RE1 is the master Routing Engine.
  Workaround:
  Before booting the card, switch over to RE0 so that it is the master Routing Engine.

- PR 840958
  Symptom:
  If the AS-MLC is plugged into the MX Series router for the first time, and no interface configurations are done on the MXC within 30 minutes, or the 10-Gigabit Ethernet interface is “shut/no shut” from the MXC, then the eight 10-Gigabit Ethernet interfaces on the router might continue to flap.
  Workaround:
  Once the links are configured and administered up from the MXC, save the configurations. Then, power-cycle the AS-MLC using the following command:

  request chassis mic fpc-slot *slot_num* mic-slot 1

  This will stabilize the links.

- PR 984878
  Symptom:
  During Media Flow Controller bootup on custom non-VXA hardware, the following message might be displayed:

  Detected CPU family 6 model 62 UNSUPPORTED HARDWARE DEVICE: CPU family 6 model > 59

  This message indicates that the Linux community has not certified the hardware. It does not mean that Media Flow Controller will not work on the hardware. This message is not applicable to VXA Series Content Engines.

  Workaround:
  We recommend that you contact Juniper Networks Customer Service before purchasing custom hardware for Media Flow Controller deployments.

- PR 1006887
  Symptom:
  When the MTU setting of the interfaces on the Application Services Modular Line Card are changed to a value other than the default (1500), sometimes the MTU setting does not take effect during a reboot.

  Workaround:
  Reconfigure the MTU setting and reboot the Application Services Modular Line Card.

Management and Logging

- **PR 743959**
  Symptom:
  When you create a bonded interface with two secondary IP addresses and modify that bonded interface, the system removes the secondary IP address.

- **PR 758556**
  Symptom:
  If you configure the SNMP community string using the CLI **snmp-server community** command with a string of length greater than 33 characters, then the SNMP query times out.

- **PR 762720**
  Symptom:
  With server-map-based namespace configurations, if the external server-map server serves chunked-encoded content, a server-map refresh and user login all occur simultaneously, and the CLI prompt will change to **CLI >**, indicating that a reduced CLI command set is available.
  - Retry the login after a period of time.
  - Avoid using chunk-encoded content for server maps.

- **PR 765271**
  Symptom:
  If multiple Media Flow Controller cache disks, filled with data, are enabled one after the other immediately after restarting the delivery service, there might be a temporary delay in the CLI session. However it is not common to do perform the following tasks in quick succession:
  - Disable all disks
  - Restart mod-delivery
  - Enable all disks

- **PR 766224**
  Symptom:
  On a bond interface with 10-Gigabit Ethernet member interfaces, the transmit queue length (txqueuelen) has the default value of 4096. This setting should be 100,000 to realize the best latency when more than 10,000 concurrent connections are expected. A txqueuelen of 100,000 is the recommended value of all 10-Gigabit Ethernet interfaces. However, on a bond interface, this is not set correctly.
  Workaround:
  Use the CLI command: **interface** ***bond interface name*** **txqueuelen 100000**. The CLI command **show network** displays the current bond interface setting.

- **PR 766520**
  Symptom:
  When you configure the access log using the **accesslog** ***logname*** **scp** CLI command, the configuration is not shown in the output from the **show running-config** command. However, the command does appear in the output from the **show accesslog** command.

- PR 766584
  Symptom:
  The cache.log shows the following message every 2 minutes when the system is idle:
  [Fri Sep 30 08:55:15.185 2011] UPDATE_ATTR "/mfc_probe:463faaa9_10.2.1.11:8080/mfc_probe/mfc_probe_object.dat" SAS dc_1 [Fri Sep 30 08:57:14 2011]
  Media Flow Controller has an internal watchdog mechanism that probes the delivery engine to make sure it is up and running. When Media Flow Controller is idle, the watchdog probes the delivery engine service by downloading a 100-KB object bypassing the cache subsystem. Because of this action, the above message appears in the cache.log. There is no functionality impact.
  Workaround:
  If you do not want to see this message, use the following CLI command in Media Flow Controller:
  namespace mfc_probe delivery protocol http origin-fetch content-store media object-size 1024001
  namespace mfc_probe object delete all

  This causes the watchdog object to be tunneled, which bypasses the caching system and does not write an entry in the cache log.

- PR 766912
  Symptom:
  When a single fully qualified object (no patterns in the fully qualified object name; that is, no pattern in the URI, directory, or filename) is deleted, Media Flow Controller guarantees object deletion when the command completes. When the object to be deleted is nonexistent, a single object delete continues to display that the object is queued for deletion.
  Workaround:
  Issue a **show namespace name object list object name** command to see if the object indeed exists. If it does, you can delete it.

- PR 767274
  Symptom:
  When Media Flow Controller serves the clients, if the user changes the access log format using the **accesslog *profile name* format *format*** CLI command, the current access log file rotates and the logs corresponding to the new format are logged in a new file. During this transition, there is a chance that a few log entries might get lost. There is no impact on data delivery to the client due to this.
  Workaround:
  Change the log format when the system is in a maintenance window to avoid this scenario.

- PR 767334
  Symptom:
  The generic virtual player's seek-mp4-type is set to “time-msec” while setting the seek-mp4-type to “time-secs” in the Web GUI. In the *Virtual Player Type Generic Configuration* page, as expected, the *Seek MP4 Type* field's combo box is populated by the two values “time-msec” and “time-secs.” However, even though the *Seek MP4 Type* is set to a time-msecs value, the GUI uses the CLI time-sec value. As a result,

Media Flow Controller does not serve the video from the client's requested seek point, even though the client sent the request with the seek query-string value in seconds.
Workaround:
Set the *Seek MP4 Type* to time-msecs under the generic virtual player using the CLI configuration mode.

- PR 767384
  Symptom:
  When setting **delivery protocol http file-type**, you must use a dot preceding the file extension. The online context help of the command shows that its enough to enter the filename extension without any preceding dot, but Media Flow Controller sets the Content-Type header only if the filename extension is configured with the preceding dot.
  Workaround:
  The filename extension must be configured with the preceding dot.

- PR 767690
  Symptom:
  When the access log format is changed and if the first request logged to the new access log file is the HTTP/0.9 request, then that entry is corrupted. With the second entry onward, it logs properly.

- PR 767708
  Symptom:
  The **accesslog *profile* object filter size *obj_size*** command should skip logging requests whose object size is less than the configured object size, but this does not work for an object size of zero (0). Zero is considered a special case and requests with the object size of zero (0) are logged.

- PR 767715
  Symptom:
  All parameters you enable for statistics sampling cannot be exported. The sampling can be enabled and used to generate alerts. The parameters listed under the **stats export csv ?** for CLI context help are only available for exporting. The following stats parameters are available for exporting as csv:

  cpu_util (CPU utilization)
  memory (Memory utilization)
  paging (Paging I/O)
  bandwidth_day_avg (Avg. Bandwidth Usage)
  bandwidth_day_peak (Peak. Bandwidth Usage)
  connection_day_avg (Avg Connection Count)
  connection_day_peak (Peak Connection Count)
  bandwidth_week_avg (Avg. Bandwidth Usage weekly)
  bandwidth_week_peak (Weekly Peak. Bandwidth Usage)
  connection_week_avg (Weekly Avg Connection Count)
  connection_week_peak (Weekly Peak Connection Count)
  bandwidth_month_avg (Monthly Avg. Bandwidth Usage)
  bandwidth_month_peak (Monthly Peak. Bandwidth Usage)
  connection_month_avg (Monthly Avg Connection Count)
  connection_month_peak (Monthly Peak Connection Count)

- PR 767744
  Symptom:

Ingest Bytes Fetched is missing from the show counters output.
Workaround:
You can use the following command to view internal counters: **show counters internal glob_tot_size_from_disk**. The counter "glob_tot_size_from_disk" counts the number of bytes delivered to a client from disk caches.

- **PR 767745**
  Symptom:
  In the **show service mod-delivery** command output, the "Dictionary generation" status listed under disk cache status is displayed as **Hardware not present** during system initialization.
  The "Dictionary generation" status shows the status of dictionary read from the disks during the startup of delivery engine service. However, during the initialization of disk cache, it is displayed as **Hardware not present**. Ignore this message until the disk cache initialization shows the status as **Ready**.

- **PR 768030**
  Symptom:
  When the Media Flow Controller cache contains a large number of objects under a namespace, because of a timing issue the CLI might return the error message "MFD subsystem not running" when you use the **show namespace *name* object list all** command.
  Workaround:
  Reissue the command and it should succeed without error.

- **PR 768041**
  Symptom:
  For each system resource statistics, there is a corresponding SNMP Object ID defined. Similarly, to report the maximum speed of a physical interface, there are two SNMP Object IDs named **ifSpeed** and **ifHighSpeed** in the IF-MIB. However, while a client gets the OID details through the SNMP protocol, these two OIDs show incorrect values for 10-Gbps physical interfaces. This issue has been addressed in Media Flow Controller Release 12.2.1 and the OID **ifSpeed** shows the value as **4294967295** even though the interface speed is more than that, and **ifHighSpeed** OID shows the speed value as **10000** correctly for 10-Gbps interfaces. Still, for bonded interfaces the above OIDs will show incorrect values. However, in the **JUNIPER-MFC-MIB::jmfcIfSpeed** OID, the values are recorded correctly for bonded and physical interfaces.
  Workaround:
  Use the **JUNIPER-MFC-MIB::jmfcIfSpeed** OID to query interface speed details.

- **PR 768054**
  Symptom:
  If you try to log in immediately after Media Flow Controller comes up after a reboot, sometimes the login might fail with a message "Management back end unavailable." If you wait a few seconds and log in again, the login succeeds. The wait time depends on the number of configurations already made to the Media Flow Controller before the reboot. There is no functional impact on the Media Flow Controller operation.
  Workaround:
  Wait a few seconds and log in to Media Flow Controller again.

- **PR 768071**

Symptom:
If a physical interface, which is a member of a bonded interface, is disabled and then enabled through the Media Flow Controller Web user interface, sometimes the interface fails to start. If this happens, then use the **configuration revert keep-basic** command to recover the interface state.

- PR 768119
  Symptom:
  When a system with bulk configuration is restarted, it can take several minutes for the CLI to come up. When a Media Flow Controller system comes up after a reboot, the configuration database is applied to the running configuration. This process can take 15 to 20 minutes for a system configured with 64 resource pools and 256 namespaces. A delay can also occur when a large configuration is applied through the Media Flow Activate interface.
  Workaround:
  If you attempt to log in immediately after a reboot, the CLI prompt might not get loaded. In this case, exit the CLI and log in again after few minutes.

- PR 768166
  Symptom:
  When the **show running-config** command is issued for the first time after a Media Flow Controller reboot, messages of type mgmtd.ERR with message string "Bail forced with error code 14000" are displayed in the syslog.
  Workaround:
  You can ignore these messages as they do not have any functional impact.

- PR 768176
  Symptom:
  When the Media Flow Controller boots up, several snmpd.ERR messages are displayed in the syslog.
  Workaround:
  You can ignore these messages as they do not have any functional impact.

- PR 768380
  Symptom:
  When you configure an IPv4 default gateway through the CLI, it overwrites the older default-gateway configurations (even though Linux accepts multiple default-gateways) so that a newly added next-hop becomes the default gateway. However, when you configure an IPv6 default gateway using the **ipv6 default-gateway** ***next hop address or interface name*** CLI command, the configurations are added and multiple default gateways are displayed in the routing table.
  Workaround:
  Always ensure that one IPv6 default gateway is configured. Verify the configuration using the **show run** CLI command. If multiple default gateways are configured, remove them using the **no ipv6 default-gateway** ***2020:2:1::101*** CLI command.

- PR 772411
  Symptom:
  When a generated SNMP trap contains a "Counter64" type varbind, **v2->v1 conversion** warning messages are logged in syslog. These messages are logged because the

underlying code tries to maintain compatibility between SNMP v1 and v2c and fails because "Counter64" is not supported in SNMP v1.
Workaround:
These messages have nothing to do with SNMP v2c. Ignore them if you are using v2c managers. Media Flow Controller is qualified for SNMP v2c only.

- **PR 774398**
  Symptom:

  When configuring MTU with a lower value for an interface, the following two issues occur:

  - While trying to configure MTU less than 68 bytes, Media Flow Controller displays an error message: "% MTU 55 for interface eth0 is out of range; must be at least 68". However, when given a value of greater than or equal to 68, it resets the value to 1280 for IPv6 support with the message: **"Interface eth0 MTU configuration changed from 99 to 1280 to support IPv6?"**
  - The Help text printed for the CLI command **interface eth0 mtu ?** does not show an acceptable value range.

- **PR 774580**
  Symptom:
  A user classified as a LogTransferUser is able to log in to the Web user interface for the Media Flow Controller. This classification of user should be to log in only using SFTP.

- **PR 775548**
  Symptom:
  The CLI allows configuration of both falling and rising error-threshold and clear-threshold for all alarms, although either threshold is applicable for a particular alarm.

- **PR 775550**
  Symptom:

  Some SNMP events and alarms tracking CPU, memory, and disk utilization are deprecated:

  - The CPU utilization events cpu-util-high, cpu-util-ok, and alarm cpu_util_indiv are deprecated. These are replaced by events aggr-cpu-util-high and aggr-cpu-util-ok triggering alarm aggr_cpu_util.
  - The memory utilization events memusage-high, memusage-ok, and alarm memory_pct_used are deprecated. These are replaced by events memutil-high, memutil-ok, and alarm nkn_mem_util.
  - The disk monitoring events disk-space-low,disk-space-ok, and alarms fs_mnt and disk_byte_rate are deprecated. The disk space monitoring can be done by events nkn-disk-space-low,nkn-disk-space-ok and alarms ssd_disk_space,sas_disk_space, sata_disk_space, and root_disk_space. The disk access bandwidth monitoring can be done by events nkn-disk-bw-high and nkn-disk-bw-ok, and alarms ssd_disk_bw, sas_disk_bw, sata_disk_bw, and root_disk_bw.

- PR 775978
  Symptom:
  Media Flow Controller allows you to refer an alias interface using both of the following commands:
  interface *ifname* **alias** *alias number*
  interface *ifname:alias number*
  However, if the configurations are applied using the **interface** *ifname:alias number* CLI command, even though the configuration database gets updated correctly (seen using the **show running-config** CLI command), the delivery engine will not listen on the alias interface.
  Workaround:
  Apply configurations to an alias interface using the **interface** *ifname* **alias** *alias number* CLI command.

- PR 776509
  Symptom:
  The SNMP DiskTable does not return the correct values for disk-caches if disk-cache is not enabled.

- PR 777424
  Symptom:
  The **<ssd|sas|sata|root>_disk_space** alarm is used to track the free disk space available in the corresponding disk tier. This is triggered if the user intentionally turns off a disk by disabling it. You can ignore this alarm incident while disabling disks.

- PR 777921
  Symptom:
  If you create multiple aliases under a loopback interface and assign an IP address from the same subnet in all of them, then one of the IP addresses deletes all other alias interfaces.
  Workaround:
  While configuring multiple alias interfaces, do one of the following:

  - Use IP addresses from different subnets.
  - Use /32, such as 255.255.255.255 as the IP subnet mask.
  - Reconfigure the alias interfaces again if you do not perform the above two workarounds and one or more alias interfaces are deleted while reconfiguring IP addresses.

- PR 778525
  Symptom:
  When Media Flow Controller is processing heavy traffic, if a new SNMP community is created sometimes the SNMP service might get restarted and continue to work after a few seconds of outage. As creation of SNMP community is normally done during the initial provisioning of Media Flow Controller without traffic, this might not be visible at deployments.

- PR 778727
  Symptom:

When an snmp-server host is added or removed using the CLI command **snmp-server *host***, the following error messages are displayed in the system log. You can ignore them.

```
May 16 04:29:42 qa05 cli[3702]: [cli.NOTICE]: user admin: Executing command: no
snmp-server host 10.157.43.182
May 16 04:29:42 qa05 snmpd[4357]: [snmpd.ERR]: duplicate registration
(jmfcNamespaceTable, jmfcNamespaceTable)
May 16 04:29:42 qa05 snmpd[4357]: [snmpd.ERR]: duplicate registration
(jmfcNamespaceHttpClientTable, jmfcNamespaceHttpClientTable)
```

- PR 781767
  Symptom:
  While installing the MaxMind GeoIP City database, Media Flow Controller also implicitly tries to open the GeoIP ISP database, and displays an error message in the system log if the GeoIP ISP database is not already installed. This error does not have any impact on the functionality and can be safely ignored:

  ```
  > May 24 10:55:28 cmbu-ixs2-1 mgmtd[7247]: [mgmtd.NOTICE]: Action initiated by
  user admin completed (44/3116)
  > May 24 10:55:54 cmbu-ixs2-1 cli[21926]: [cli.NOTICE]: user admin: Executing
  command: application maxmind install GeoIPCity.dat.gz
  > May 24 10:55:54 cmbu-ixs2-1 geodbd[8197]: [geodbd.NOTICE]: Got the install action
   for /nkn/maxmind/downloads/GeoIPCity.dat.gz
  > May 24 10:55:55 cmbu-ixs2-1 pm[7243]: [pm.NOTICE]: Output from geodbd
  (GEODBD) (pid 8197): Error Opening file /nkn/maxmind/db/GeoIPISP.dat
  ```

- PR 782739
  Symptom:

  An external user can pull service logs from Media Flow Controller through SFTP using two modes:

  - **Password-less login**—Used by remote users configured as trusted users in Media Flow Controller using the **ssh client user LogTransferUser authorized-key sshv2 *key*** CLI command.
  - **Password-based login**—Used by remote users not configured as trusted users in Media Flow Controller. Enable this login mode by setting a password for LogTransferUser in Media Flow Controller.

  The "Account status" field displayed by the **show usernames** command displays only the status of the password-based login. So if a deployment configuration uses only password-less login, the **show usernames** shows **Local password login disabled** which should not be misinterpreted as the remote user cannot log in to Media Flow Controller through SFTP to pull logs.

  To know whether a remote user is configured for password-less login, use the **show ssh client** CLI command. If the authorized-key corresponding to the remote user is displayed, it means the remote user can pull logs from Media Flow Controller through SFTP.

- PR 785508
  Symptom:

Media Flow Controller allows you to designate the list of interfaces to use as delivery interfaces. The bandwidth for the global resource pool is assumed based on the bandwidth available across all the designated delivery interfaces. If an alias interface is designated as a delivery interface using the CLI command **delivery protocol http interface *interface*** and the corresponding physical interface is not in the delivery interface list, the bandwidth is not assumed by the global resource pool.
Workaround:
While adding an alias interface to the delivery interface list, also add the corresponding physical interface to the list. This is not an issue if you do not explicitly designate an interface and delivery interface. In this case, all available interfaces are considered to be delivery interfaces.

- **PR 786173**
  Symptom:
  By default, LogTransferUser should be in "Account Disabled" state instead of "Local password login disabled."

- **PR 789476**
  Symptom:
  Even though the Media Flow Controller CLI allows you to configure multiple bonded interfaces, considering issues in handling multiple bonded interfaces internally, it is recommended to use only one bonded interface with a maximum of two 10-gigabyte members.

- **PR 789644**
  Symptom:
  You MUST use the LogTransferUser login only for downloading or pulling log files from Media Flow Controller. The current infrastructure allows you to upload a file or delete a file from the log folders. However you should not upload any files to the log folders or delete the existing files from the log folders. This action is handled automatically by Media Flow Controller. Doing it externally might affect Media Flow Controller logging functionality.

- **PR 789862**
  Symptom:
  Once you insert a JBOD shelf to an online Media Flow Controller, a few operations that require massive system resources must be done on each of the disks attached to the JBOD and the system might go sluggish or even be unresponsive for a few minutes. It is recommended to attach or detach JBODs to Media Flow Controller during maintenance windows. If the system becomes unresponsive, a reboot brings it up to normal working condition.

- **PR 791224**
  Symptom:
  The second and subsequent requests from a persistent connection logs **Invalid IP** against the %Y field in the access log.

- **PR 792454**
  Symptom:
  When you have multiple IP addresses in the same subnet as the management IP address, to direct the management traffic to use a specific IP addresses as the source IP address, use the CLI command **management ip route *network mask* gateway *ip address***

source *ip address*. However, if you want to reconfigure the CLI, just entering the new values again will not ensure the existing values are properly overridden. Use the **no management ip route *network mask* gateway *ip address* source *ip address*** CLI command to explicitly disable the configuration before configuring the new values.

- PR 798218
  Symptom:
  If a server-map is associated with a namespace, and if the user wants to convert the namespace to a non server-map associated namespace, then just overwriting the **namespace *name* origin-server** CLI will not disassociate the existing server-map.
  Workaround:
  You must explicitly disassociate the server-map using the **no namespace *name* origin-server server-map** CLI command.

- PR 798892
  Symptom:
  With Media Flow Controller Release 12.2.1, necessary web services must be enabled, otherwise the upgrade to 12.1.0 from a previous release fails. The following web configuration should be present if mod-dmi is enabled:
  web enable
  web http enable
  web http port 8080
  no web http redirect
  web httpd listen enable
  web https enable
  Apart from the above configuration, web httpd should not listen on any interfaces for mod-dmi to work properly.

- PR 799014
  Symptom:
  Under rare conditions, the object delete/list might display a Python exception **OSError: [Errno 10] No child processes** on the CLI. This happens due to a limitation in the current version of Python used in Media Flow Controller, and will be fixed in future releases. There is no functional impact due to this issue. The exception occurs only after the object list/delete is completed.

- PR 801803
  Symptom:
  The addition and removal of access log profiles is normally done during the initial provisioning of the Media Flow Controller and during a maintenance window. However if you remove or add access log profiles when the system is serving traffic, the logging service might restart. The service immediately returns to normal, and there is no functionality impact.

- PR 805761
  Symptom:
  In newly installed Media Flow Controllers, configuration of namespaces sometimes fails at the namespace activation stage. While the problem is intermittent, it can be avoided by restarting the Media Flow Controller delivery engine when basic configurations such as license installation and the configuration of IPs on the interfaces are complete, and then configuring the namespaces.

- **PR 803551**
  Symptom:
  If a URI with a question mark (?) in the name is cached in Media Flow Controller, you cannot list or delete that name by specifying the **?** as a string in the search pattern, because it is considered to be a metacharacter.
  For example, if you have a URI **/a/b/c?d=e** cached under **namespace *name***, then **namespace *name* object list /a/b/c?d=e** does not list the URI.
  Workaround:
  Use other metacharacters to replace the **?** in the URI name when listing it.

- **PR 821791**
  Symptom:
  When no mail server is configured, **/nkn/ftphome/root/dead.letters** fills up with auto-generated e-mails causing **/nkn to be** 100 percent full.
  Workaround:
  Use the following command to disable dead mail generation:
  no email dead-letter enable

- **PR 834313**
  Symptom:
  A **jmfcDiskSpaceLow** trap or e-mail notification is generated whenever the free disk space of a particular cache-disk or root-disk falls below the configured threshold. This event, trap, or e-mail notification will not be functional for Release 12.3.*x*.

- **PR 837708**
  Symptom:
  The dashboard's daily interface bandwidth graph plot values are sampled every 300 seconds, while the weekly interface bandwidth plot values are sampled every 1800 seconds. However while plotting the graph, the cumulative values are plotted instead of the rate. For example, if we send 12 Mbps of continuous traffic for a week, the daily graph shows 3600 MB, and the weekly graph shows 216,000 MB, which is the cumulative of all samples.

- **PR 907377**
  Symptom:
  In a system where traffic is served for a long time, under rare conditions, the **reload** command might not reload the system immediately.

  Workaround:
  Perform the following commands to reboot the system:

  1. Start the Media Flow Controller shell.

     _shell

  2. Restart the process management service.

     service pm restart

Network Subsystem

- **PR 869368**
  Symptom:
  If fast start is enabled in a virtual player, then the initial data of the video URI served through the associated namespace will be delivered without bandwidth throttling. However, if the associated namespace has a client driven cache-fill scheme, then the first time download rate of the URI from the origin will be capped at 128KBps. This limit will not affect subsequent client requests for which the data is served from the cache. If the namespace is configured for an aggressive cache fill scheme, then this limit will not be visible.

Reverse Proxy

- **PR 696896**
  Symptom:
  If you are using the reverse proxy service and you modify the HTTP origin field from the origin map to a fully qualified domain name (FQDN), the reprovision fails.
- **PR 742908**
  Symptom:
  When you provision three Media Flow Controllers with 256 namespaces (and 64 resource pools), the CPU of the Media Flow Controller goes to 100 percent. You cannot execute any CLI commands until the provisioning activities are complete.
- **PR 763177**
  Symptom:
  The Media Flow Controller does not support the definition of origin fetch policies when the origin is an NFS origin server.
- **PR 763459**
  Symptom:
  Resource pool-based bandwidth limit does not work for traffic that is tunneled to the origin server. However, a resource pool-based connection limit does work.
- **PR 763644**
  Symptom:
  AFR is not honored if Media Flow Controller tunnels the request based on request attributes.
- **PR 763693**
  Symptom:
  The origin selection policy is not functional when the origin-escalation map or cluster map is configured in a namespace. If you configure an origin-escalation map or cluster map in a namespace and if you set an origin server using Policy Engine, the request is still forwarded to the origin nodes configured in the server map.
  Workaround:
  We recommended that you do not use any policy rules to set an origin server when a server map is defined in the namespace.
- **PR 764818**
  Symptom:

Idle connections from the client are not accounted for by the client-session parameter allocated to a resource pool. While restricting the number of connections opened by clients belonging to a particular resource pool, Media Flow Controller does not account for idle sessions. Idle connections are not bound to a namespace and hence are not accounted for when tracking resource usage at a namespace and resource pool level. However, the idle connections are accounted for towards the network-level admission control configured by the **network connection concurrent session** CLI command. If the idle sessions increase, it might reduce the effective number of active connections that a system can handle. Connections can appear to be rejected even though the resource pool usage shows available connections, because the rejection is caused by the network connection concurrent session setting and not the resource pool configuration.
Workaround:
Do not allocate all available open connections to resource pools. Leave the expected idle sessions worth of client sessions in the global resource pool. These balance the number of sessions consumed by idle sessions, and the resource pools can still support available active sessions.

- PR 764962
  Symptom:
  When you configure a client-side policy to override a cache-control:no-cache directive from a client using Policy Engine, and the client sends a cache-control:no-cache directive that disallows caching the content into a cache, the Media Flow Controller overrides that directive and caches the content. This scenario is the case for content with fixed length that comes with a content-length. The Media Flow Controller does not honor this policy for chunked encoded content.
  Workaround:
  To override the client's cache-control:no-cache directive and to cache the content even if the response is chunked encoded, apply the policy at the pe_om_recv_response point.

- PR 767400
  Symptom:
  Policy engine header manipulation actions at the **pe_http_send_response** side are not applied if the SSL request matches a plain-text delivery namespace. If an SSL request matches a plain-text delivery namespace, then that request is rejected with a 403-52032 error code. The header manipulation actions applied at the Policy Engine's **pe_http_send_response** side are not applied for this type of request.

- PR 767602
  Symptom:
  The load feedback API daemon listens for load feedback requests with port 2010 on all available interfaces in Media Flow Controller. Because this port is an unsecured port on the data interfaces, it is potentially open to DoS attacks.
  Workaround:
  Ensure that upstream network devices are configured to block traffic from any external interface on port 2010. This port should only be used by known devices within your network.

- PR 767622
  Symptom:

The origin escalation feature and the DNS-based origin failover feature are not designed to work together. If both features are configured at the same time, then the origin escalation feature configures the first available IP address for the domain; if the first available IP address is down, then the client is served with a 504 response code.

- PR 767624
  Symptom:
  If a namespace ***name1*** is inherited into another namespace **name2**, and if Content Ingest Manager traffic hits **name2**, the Content Ingest Manager log logs **name1** as **namespace *name*** even though the current active **namespace *name*** is **name2**. There is no impact on data delivery.
  Workaround:
  Map **name1** to **name2** while doing any analysis on the Content Ingest Manager crawl log.

- PR 767692
  Symptom:
  During the Content Ingest Manager crawling process, if the origin server is configured to send a 302 response code to the client's request, even if it is redirected to follow a 302 response code configured in namespace, then the Media Flow Controller does not follow the 302 response code and crawl add fails.

- PR 767717
  Symptom:
  Media Flow Controller utilizes 100 percent CPU while crawling a directory with more than 50,000 URIs.

  When the crawling directory contains a large number of URIs, such as 50,000 URIs for example, origin server sends the index.html as the chunked response of the 100 percent CPU utilization.
  Workaround:
  None. The crawled base URL response from the origin server must not come as a chunked response. The number of URLs must be limited.

- PR 767750
  Symptom:
  If the listen port of the load feedback system is modified, it is not reflected in the existing instance of the daemon.
  Workaround:
  Restart the load feedback service using the CLI command **pm process lfd restart** to reflect the change.

- PR 767798
  Symptom:
  When Content Ingest Manager crawls an origin and an object fails to be ingested for any reason, that object will also not be ingested in subsequent crawls.

- PR 767873
  Symptom:
  If there are many namespaces and resource pools configured in the system when the delivery service comes up after a restart, then the initialization of the delivery service takes a little longer than expected. In the meantime, internal processes trying to connect

to the delivery service might report failure and try again to connect. The **show service mod-delivery** command output will have “Num Failures“ as a non-zero value. This can be ignored as there is no impact of this scenario in the functioning of Media Flow Controller.

- PR 767891
  Symptom:
  Content Ingest Manager crawling does not occur if the namespace is configured with **ip-version follow-client** CLI command in the origin configuration.

- PR 768116
  Symptom:
  Common name verification during SSL server authentication in Media Flow Controller is mandatory.

  Issues occur if an IP address is used as the origin server name or if the origin server does not support Server Name Indication (SNI).

- PR 768165
  Symptom:
  The Content Ingest Manager crawl instance can get stuck if the delivery application is restarted when the crawl instance is in progress. If the delivery application is restarted when the current crawl instance is in progress, on rare occasions the crawl instance can stop crawling. This only occurs for the current crawl instance and the crawl starts again at the next refresh interval.
  Workaround:
  If the refresh interval is shorter, wait for the refresh interval to lapse; otherwise, change the crawl start time to the current time and trigger the Content Ingest Manager crawl again.

- PR 768294
  Symptom:
  While caching URIs with a query string using the pre-fetch feature, Media Flow Controller truncates the query string portion and caches the URIs without query strings. This can lead to a scenario where a cache collision occurs if multiple URIs differentiated only by a query string are queued using pre-fetch.

- PR 773772
  Symptom:
  The Media Flow Controller CLI accepts Policy Engine scripts with a single-character name, but the policies applied through the script are not taken into account.
  Workaround:
  Name the Policy Engine scripts with at least two characters.

- PR 785290
  Symptom:
  If you configure the cluster map with a hostname instead of an IP address and link it with a namespace, the watchdog starts to continuously restart the core caching engine when you manually perform a mod-delivery restart.

- PR 787911
  Symptom:

The connection pool feature in Media Flow Controller allows a request towards origin to reuse a connection created by a previous request to origin. In case of HTTPS origin, if a GET request is made to the origin and the connection is added to the reuse pool, the connection will not be used by another revalidation request to the same origin. However, if the next request is another GET request, the connection will be reused. Connection reuse across regular GET requests and revalidation requests happens without issues in case of HTTP origin.

- **PR 789455**
  Symptom:
  The maximum support length for a Content Ingest Manager crawler name is 16 characters. If you try to configure a lengthy crawler name (greater than 16 characters), Media Flow Controller displays the error “Error creating crawler profile.”

- **PR 790795**
  Symptom:
  Some origin servers do not support HTTP byte range requests. In such cases, Media Flow Controller is not able to support seek and scrub requests due to the fact that byte range requests triggered by Media Flow Controller result in the full file being delivered by the origin.
  Workaround:
  For those web sites whose origin servers do not support byte ranges, set seek to tunnel mode in Media Flow Controller.

Transparent and Reverse Proxy

- **PR 693511**
  Symptom:
  Provisioning the transparent and reverse proxy services fails if that service is associated with any virtual players containing the shared secret that is only an equal sign (**=**).
  Workaround:
  Do not use an equal sign (**=**) as the sole shared secret on any virtual players. If the shared secret contains other alphanumeric characters, there are no problems.

Transparent Proxy

- **PR 766437**
  Symptom:
  When you boot Media Flow Controller, the following message appears in the system log:
  Apr 4 09:12:37 mfc-unconfigured-7223e2 mgmtd[5396]: [mgmtd.WARNING]: Bad target name "TPROXY" under rule /iptables/state/table/mangle/chain/PREROUTING/rule/1
  Workaround:
  None. These messages are harmless, and you can ignore them.

- **PR 787718**
  Symptom:
  To switch from **namespace *name* origin-server http follow dest-ip use-client-ip** to **namespace *name* origin-server http follow header Host use-client-ip**, the functionality still reflects **namespace *name* origin-server http follow dest-ip use-client-ip** mode.
  Workaround:

Apply the **namespace *name* origin-server http follow header Host use-client-ip** CLI command twice to switch to the **follow header host use-client-ip** from **follow dest-ip use-client-ip** mode.

Documentation Updates

Media Flow Controller License No Longer Required

- Throughout the Media Flow documentation remove mention of the Media Flow Controller licenses. See the "Media Flow Controller License Is No Longer Required" section of these release notes.

New CLI Commands Introduced in Media Flow Controller Release 12.3.8

The following CLI commands are introduced with Media Flow Controller Release 12.3.8.

Content Ingest Manager

- **crawler *name* action x-domain crawl**
- **crawler *name* no action x-domain crawl**

DPI Filtering (Transparent Proxy)

- **clear log-analyzer filter-rules *device-map-name***
- **device-map *name***
- **device-map *name* filter-configuration frequency *minutes***
- **device-map *name* filter-configuration max-rules *number***
- **device-map *name* fqdn *fqdn***
- **device-map *name* username *username* password *password***
- **log-analyzer config-file local-file**
- **log-analyzer config-file url *url***
- **log-analyzer target *device-map-name***
- **log-analyzer target *device-map-name* command-mode batch-file**
- **log-analyzer target *device-map-name* command-mode inline**
- **no device-map *name***
- **no log-analyzer target *device-map-name***
- **show device-map *name***
- **show log-analyzer target *device-map-name***

URL Filtering

- delivery protocol http filter mode packet
- delivery protocol http filter mode proxy
- delivery protocol http no filter
- filter-map *map-name* crypto-key *key*
- filter-map *map-name* file-url *url* format-type calea
- filter-map *map-name* file-url *url* format-type iwf
- filter-map *map-name* file-url *url* format-type url-list
- filter-map *map-name* refresh-force
- filter-map *map-name* refresh-interval *hours*
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action 200-ok *text*
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action 301-redirect *fqdn*
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action 301-redirect *fqdn uri*
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action 302-redirect *fqdn*
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action 302-redirect *fqdn uri*
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action 403-forbidden
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action 404-not-found
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action close-conn
- namespace *name* delivery protocol http client-request filter (black-list *filter-map-name* | max-uri-size *size* | white-list *filter-map-name*) action reset-conn
- namespace *name* delivery protocol http no client-request filter
- namespace *name* delivery protocol http no client-request filter (black-list | white-list)
- namespace *name* no delivery protocol http client-request filter
- namespace *name* no delivery protocol http client-request filter (black-list | white-list)
- no delivery protocol http filter
- no filter-map *map-name*
- no namespace *name* delivery protocol http client-request filter
- no namespace *name* delivery protocol http client-request filter (black-list | white-list)

- **show filter-map list**
- **show filter-map** *map-name*

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

Revision History

4 February 2015—Revision 3, Media Flow Controller 12.3.8

22 December 2014—Revision 2, Media Flow Controller 12.3.8

3 October 2014—Revision 1, Media Flow Controller 12.3.8