What's new in v4.2.x

These are the highlights of new features or additions to existing features in v4.2.x.

Websockets support

LinkedIn recently donated an implementation that allows for proxying of WebSockets. It supports the basic upgrade path for a web socket, and is configured using normal remap.config rules:

```
map ws://www.example.com  ws://ws.example.com:9090
```

This is still slightly in "experimental" mode, so we're definitely looking forward to hear feedback from people using this.

Jira: TS-2541

ICP support

Traffic Server has had an ICP module for the longest time, which unfortunately has been non-functional. Recent efforts have reactivated this feature again! The same configurations as before applies, nothing has changed in behavior or configuration.

Jira: TS-32

New configuration option for attaching server sessions to client sessions

Even though Traffic Server always supported sharing origin server sessions between client sessions, a server session would by default be associated with a Keep-Alive client session for the duration of that client session. This was configurable by limiting the number of server connections (*proxy.config.http.server_max_connections*). To decouple this overloaded semantics, a new configuration option has been created:

```
CONFIG proxy.config.http.attach_server_session_to_client INT 0
```

The default is "0", which means we no longer attach the server sessions to the client by default. This is a change from previous versions of Apache Traffic Server, but it's a reasonable change since it changes what should be considered a broken behavior. Changing this configuration to "1" will not restore the old behavior, but will instead always attach the server sessions regardless of what *proxy.config.http.server_max_connections* is set to.

Jira: TS-2422

SSL new features and improvements

Change in behavior of proxy.config.ssl.server.honor_cipher_order setting

A bug regarding the behavior of the proxy.config.ssl.server.honor_cipher_order setting has been fixed. When enabled this setting allows the server to pick the preferred cipher used during the TLS or SSLv3 handshake based on the value of the proxy.config.ssl.server.cipher_suite setting.

Previously, a value of 0 enabled this setting, and a value of 1 disabled this setting - the reverse of the expected behavior. ATS previously shipped with a value of 1 (disabled). Starting in 4.2.0, the expected behavior was restored - 1 for enable, 0 for disable. The default in 4.2.0+ is 0, so the out of the box behavior remains the same.

Please verify/update records.config if you migrated this value from an older version of ATS to 4.2.0.

Jira: TS-2370

TLS 1.1 and 1.2 Configurations

There are two new options to turn off or on TLS 1.1 and TLS 1.2. By default TLS 1.2 is enabled still (value of 1), but can be disabled if you experience a crash with TLS 1.2. These versions of OpenSSL would experience this problem: 1.0.1, 1.0.1a, 1.0.1b, 1.0.1c, 1.0.1d, and 1.0.1 e. There is an open issue with openssl http://rt.openssl.org/Ticket/Display.html?id=3200.

Update: January 10, 2014 - The openssl issue with TLS 1.2 has been resolved in openssl 1.0.1f (you can enable TLS 1.2 if you update openssl to 1.0.1f). More information is available at http://www.openssl.org/news/vulnerabilities.html#2013-6449 regarding this vulnerability (CVE-2013-6449).

```
CONFIG proxy.config.ssl.TLSv1_1 INT 1
CONFIG proxy.config.ssl.TLSv1_2 INT 1
```

Jira: TS-2355

RFC 5077 TLS Session tickets

For supporting RFC 5077 TLS Session tickets across a ATS cluster, all the machines need to have the same server ticket. This adds two new configurations to ssl_multicert.config:

```
ssl_ticket_enabled=1|0
ticket_key_name=<filename>
```

Jira: TS-1146

Support for HSTS (HTTP Strict Transport Security)

From WikiPedia: The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion. Two new configuration option, which is overridable per remap rule, has been added to Traffic Server:

```
CONFIG proxy.config.ssl.hsts_max_age INT -1
CONFIG proxy.config.ssl.hsts_include_subdomains INT 0
```

Jira: TS-1668

Change in ordering for SSL certificates with same CN

Previous to 4.2.x, for two SSL certificates with the same CN, the last one would be used. This has been changed to properly using the first one as well as issuing a warning about the situation. This will only affect those with multiple SSL Certificates with the same CN, for example a self-signed one and one from a CA.

Configure max TLS record size

The client can decipher the data only once it has received a full record over SSL. The record size can have significant impact on the page load time performance of the application. No limitation on record size means that clients might have to download up to 16KB of data before starting to process them, whereas very small records incur a larger overhead due to record framing. A new configuration has been added to control this:

```
CONFIG proxy.config.ssl.max_record_size INT 0
```

Jira: TS-2365

Add forward secrecy support

Added support for elliptic curve ciphers (http://en.wikipedia.org/wiki/Elliptic_curve_cryptography) which generates a new key per session for enhanced security. To use the elliptic curve ciphers you will need to modify the cipher list with the appropriate ciphers. For example:

```
CONFIG proxy.config.ssl.server.cipher_suite STRING ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-
AES256-SHA384:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-RSA-RC4-SHA:ECDHE-
RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:RC4-SHA:RC4-MD5:AES128-SHA:AES256-SHA:
DES-CBC3-SHA:!SRP:!DSS:!PSK:!aNULL:!eNULL:!SSLv2
```

Jira: TS-2372

Release memory for idle SSL sessions

OpenSSL tends to allocate about 50KB of memory for each connection. Setting flag: "SSL_MODE_RELEASE_BUFFERS" can save around 34K per idle SSL connection. This flag has no effect on SSL v2 connections, or on DTLS connections. ref: http://www.openssl.org/docs/ssl/SSL_CTX_set_mode.html .

Jira: TS-2413

Configurable TLS session timeout threshold

Default is 300 seconds. It's good to be configurable so that application can specify the threshold for the expiration of internal session and session ticket. Therefore, this is now configurable with the following configuration option:

```
CONFIG proxy.config.ssl.session_cache.timeout INT 0
```

Jira: TS-2416

Gentoo Layout changes

Runtimedir on Gentoo changed from /var/run to /run

New options for traffic_line

A couple of management options were added to traffic_line, which previously required the use of traffic_shell:

```
root@cosmo 421/0 # traffic_line --status
Proxy -- on
root@cosmo 422/0 # traffic_line --clear_alarms all
No Alarms to resolve
root@cosmo 423/0 # traffic_line --alarms


No active alarms.
```

Jira: TS-2533

More details

- Slide deck with more feature / improvement details

If you experience issues

Please take a look at TS-2564 to see if this issue is affecting you.