D4Science Infrastructure - Task #12443

Task # 12425 (Closed): Enable TLS/SSL on the mongodb clusters

Enable TLS/SSL on the mongodb development cluster

Sep 10, 2018 03:29 PM - Roberto Cirillo

Status:	Closed	**Start date:**	Sep 10, 2018
Priority:	Normal	**Due date:**	
Assignee:	_InfraScience Systems Engineer	**% Done:**	100%
Category:	System Application	**Estimated time:**	0.00 hour
Target version:	Mongodb: enable and enforce TLS		
Infrastructure:	Development, Pre-Production		

Description

It's supported since 3.0 and the configuration seems straightforward.

The documentation: https://docs.mongodb.com/v3.4/tutorial/configure-ssl/
How to upgrade a cluster to tls/ssl: https://docs.mongodb.com/v3.4/tutorial/upgrade-cluster-to-ssl/

Documentation for the clients: https://docs.mongodb.com/v3.4/tutorial/configure-ssl-clients/

Related issues:

Blocks D4Science Infrastructure - Task #12444: Enable TLS/SSL on the mongodb ...	**Closed**	**Sep 10, 2018**
Blocked by D4Science Infrastructure - Task #12445: SSL Certificate for mongod...	**Closed**	**Sep 10, 2018**

History

#1 - Sep 10, 2018 03:31 PM - Roberto Cirillo

- Blocks Task #12444: Enable TLS/SSL on the mongodb production cluster added

#2 - Sep 10, 2018 04:01 PM - Roberto Cirillo

- Blocked by Task #12445: SSL Certificate for mongodb development cluster added

#3 - Sep 13, 2018 12:04 PM - Roberto Cirillo

- Status changed from New to In Progress

I'm going to test the new settings on mongo5-d-d4science.org that is running in standalone mode. If it works properly with the client libraries (with and without ssl enabled), I'm going to deploy the new settings on the whole development cluster.

#4 - Sep 13, 2018 02:57 PM - Roberto Cirillo

- Status changed from In Progress to Paused

#5 - Sep 18, 2018 11:59 AM - Roberto Cirillo

- Status changed from Paused to In Progress

#6 - Sep 18, 2018 12:19 PM - Roberto Cirillo

- Status changed from In Progress to Paused

- % Done changed from 0 to 20

#9 - Sep 20, 2018 10:58 AM - Roberto Cirillo

- Status changed from Paused to In Progress

#11 - Sep 20, 2018 06:22 PM - Roberto Cirillo

- Status changed from In Progress to Closed

- % Done changed from 20 to 70

The development cluster is working fine with ssl. I've also enabled ssl on volatile instance
Now, each node is running in **allowSSL** mode, this setting allows the node to accept both TLS/SSL and non-TLS/non-SSL incoming connections. Its

connections to other nodes do not use TLS/SSL. .

Next step is to use the ssl mode: **preferSSL**. In this case each node accepts both TLS/SSL and non-TLS/non-SSL incoming connections, and its connections to other nodes use TLS/SSL. Last step is to use the mode **requiredSSL** where the cluster will reject any non-TLS/non-SSL connections.

#12 - Sep 24, 2018 10:12 AM - Roberto Cirillo

- Status changed from Closed to In Progress

#13 - Sep 24, 2018 10:14 AM - Roberto Cirillo

- Status changed from In Progress to Paused

#14 - Sep 25, 2018 11:37 AM - Roberto Cirillo

- Status changed from Paused to In Progress

I've tried to switch the cluster configuration from allowSSL to preferSSL but I see the following error on the primary node. At this time all the secondary members were switched to preferSSL:

```
2018-09-25T11:04:09.106+0200 I NETWORK  [conn20603] SSL mode is set to 'preferred' and connection 20603 to 146
.48.1
23.1:60626 is not using SSL.
2018-09-25T11:04:09.123+0200 I ACCESS   [conn20603] Successfully authenticated as principal __system on local
2018-09-25T11:04:09.124+0200 I -        [conn20603] end connection 146.48.123.1:60626 (4 connections now open)
2018-09-25T11:04:09.130+0200 I NETWORK  [thread1] connection accepted from 146.48.123.1:60629 #20604 (4 connec
tions
 now open)
2018-09-25T11:04:09.131+0200 I NETWORK  [conn20604] SSL mode is set to 'preferred' and connection 20604 to 146
.48.1
23.1:60629 is not using SSL.
2018-09-25T11:04:09.131+0200 I NETWORK  [conn20604] received client metadata from 146.48.123.1:60629 conn20604
: { d
river: { name: "NetworkInterfaceASIO-Replication", version: "3.4.15" }, os: { type: "Linux", name: "Ubuntu", a
rchit
ecture: "x86_64", version: "14.04" } }
2018-09-25T11:04:09.136+0200 I ACCESS   [conn20604] Successfully authenticated as principal __system on local
2018-09-25T11:04:09.675+0200 I NETWORK  [thread1] connection accepted from 146.48.123.72:41183 #20605 (5 conne
ction
s now open)
2018-09-25T11:04:09.716+0200 E NETWORK  [conn20605] SSL peer certificate validation failed: certificate not tr
usted
2018-09-25T11:04:09.717+0200 I -        [conn20605] end connection 146.48.123.72:41183 (5 connections now open
)
2018-09-25T11:04:09.737+0200 I NETWORK  [thread1] connection accepted from 146.48.123.72:41185 #20606 (5 conne
ction
s now open)
2018-09-25T11:04:09.778+0200 E NETWORK  [conn20606] SSL peer certificate validation failed: certificate not tr
usted
2018-09-25T11:04:09.779+0200 I -        [conn20606] end connection 146.48.123.72:41185 (5 connections now open
)
2018-09-25T11:04:09.799+0200 I NETWORK  [thread1] connection accepted from 146.48.123.72:41187 #20607 (5 conne
ction
s now open)
2018-09-25T11:04:09.840+0200 E NETWORK  [conn20607] SSL peer certificate validation failed: certificate not tr
usted
2018-09-25T11:04:09.840+0200 I -        [conn20607] end connection 146.48.123.72:41187 (5 connections now open
)
```

#15 - Sep 25, 2018 12:09 PM - Roberto Cirillo

- Assignee changed from Roberto Cirillo to _InfraScience Systems Engineer

I think there is a problem with our sslCAFile.
As reported here: https://jira.mongodb.org/browse/SERVER-21003
The CAFile should contain the root certificate chain from the Certificate Authority.
Please, @andrea.dellamico@isti.cnr.it could you verify that?

#16 - Sep 25, 2018 08:08 PM - Andrea Dell'Amico

- Assignee changed from _InfraScience Systems Engineer to Roberto Cirillo

Well, if it's what they want... I just changed the playbook so that by default it uses the DST_Root_CA_X3 CA file, the one that signs the Letsencrypt CA. It's on the file system already, so the configuration will point to that file.

I pushed the change, the playbook must be run again on all the hosts to change the configuration. If you want to make the change manually, the CA file path is /usr/share/ca-certificates/mozilla/DST_Root_CA_X3.crt.
So the configuration line becomes

```
CAFile: /usr/share/ca-certificates/mozilla/DST_Root_CA_X3.crt
```

#17 - Sep 26, 2018 10:33 AM - Roberto Cirillo

- Assignee changed from Roberto Cirillo to _InfraScience Systems Engineer

This change doesn't work. Now I see this error server side when I try to connect to the mongo by my client:

```
2018-09-26T10:25:16.123+0200 I -        [conn3] end connection 146.48.85.73:52530 (1 connection now open)
2018-09-26T10:25:16.623+0200 I NETWORK  [thread1] connection accepted from 146.48.85.73:52532 #4 (1 connection
 now open)
2018-09-26T10:25:16.628+0200 E NETWORK  [conn4] SSL: error:14094416:SSL routines:SSL3_READ_BYTES:sslv3 alert c
ertificate unknown
2018-09-26T10:25:16.628+0200 I -        [conn4] end connection 146.48.85.73:52532 (1 connection now open)
2018-09-26T10:25:17.128+0200 I NETWORK  [thread1] connection accepted from 146.48.85.73:52534 #5 (1 connection
 now open)
2018-09-26T10:25:17.131+0200 E NETWORK  [conn5] SSL: error:14094416:SSL routines:SSL3_READ_BYTES:sslv3 alert c
ertificate unknown
2018-09-26T10:25:17.131+0200 I -        [conn5] end connection 146.48.85.73:52534 (1 connection now open)
2018-09-26T10:25:17.632+0200 I NETWORK  [thread1] connection accepted from 146.48.85.73:52536 #6 (1 connection
 now open)
2018-09-26T10:25:17.635+0200 E NETWORK  [conn6] SSL: error:14094416:SSL routines:SSL3_READ_BYTES:sslv3 alert c
ertificate unknown
2018-09-26T10:25:17.635+0200 I -        [conn6] end connection 146.48.85.73:52536 (1 connection now open)
2018-09-26T10:25:18.137+0200 I NETWORK  [thread1] connection accepted from 146.48.85.73:52538 #7 (1 connection
 now open)
2018-09-26T10:25:18.139+0200 E NETWORK  [conn7] SSL: error:14094416:SSL routines:SSL3_READ_BYTES:sslv3 alert c
ertificate unknown
2018-09-26T10:25:18.140+0200 I -        [conn7] end connection 146.48.85.73:52538 (1 connection now open)
2018-09-26T10:25:18.640+0200 I NETWORK  [thread1] connection accepted from 146.48.85.73:52540 #8 (1 connection
 now open)
2018-09-26T10:25:18.643+0200 E NETWORK  [conn8] SSL: error:14094416:SSL routines:SSL3_READ_BYTES:sslv3 alert c
ertificate unknown
2018-09-26T10:25:18.643+0200 I -        [conn8] end connection 146.48.85.73:52540 (1 connection now open)
```

If I've understood correctly, as reported in the link present in my previous comment, the root certificate should be added to the CA file, not replace the CAFile.

#18 - Sep 26, 2018 12:48 PM - Roberto Cirillo

- % Done changed from 70 to 90

#20 - Sep 26, 2018 04:57 PM - Andrea Dell'Amico

- Status changed from In Progress to Feedback

I changed the playbook so that it builds the CAfile adding both the root CA and the intermediate one. To ensure that the playbook does its job correctly, the file /etc/pki/mongodb/lets-encrypt-x3-cross-signed.pem must be removed from the hosts.

#21 - Oct 01, 2018 03:15 PM - Roberto Cirillo

I've tried to delete the following file: /etc/pki/mongodb/lets-encrypt-x3-cross-signed.pem
and re run the playbook but it fails with the following error:

```
TASK [../library/roles/mongodb-org : Add the Root CA certificate to the mongodb CA file] ********************
*************************************************************************************************************
***********
fatal: [mongo5-d-d4s.d4science.org]: FAILED! => {"changed": true, "cmd": ["cat", "/usr/share/ca-certificates/m
ozilla/DST_Root_CA_X3.crt", ">>", "/etc/pki/mongodb/lets-encrypt-x3-cross-signed.pem"], "delta": "0:00:00.0090
90", "end": "2018-10-01 15:04:25.794398", "msg": "non-zero return code", "rc": 1, "start": "2018-10-01 15:04:2
5.785308", "stderr": "cat: >>: No such file or directory", "stderr_lines": ["cat: >>: No such file or director
y"], "stdout": "-----BEGIN CERTIFICATE-----\nMIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/\
nMSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT\nDkRTVCBSb290IENBIFgzMB4XDTAwMDkzMDIxMTIxOVo
XDTIxMDkzMDE0MDExNVow\nPzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1cmUgVHJ1c3QgQ28uMRcwFQYDVQQD\nEw5EU1QgUm9vdCBDQSBYM
zCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB\nAN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4O\
nrz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEq\nOLl5CjH9UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGii
fSKOeDNoJjj4XLh7dIN9b\nxiqKqy69cK3FCxolkHRyxXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw\n7BZy1SbsOFU5Q9D8/RhcQ
PGX69Wam40dutolucbY38EVAjqr2m7xPi71XAicPNaD\naeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNV\
nHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQMA0GCSqG\nSIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9
LwwmglSBd49lZRNI+DT69\nikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXr\nAvHRAosZy5Q6XkjEGB5YG
```

V8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZz\nR8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5\nJDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubSfZGL+T0yjWW06XyxV3bqxbYo\nOb8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ\n-----END CERTIFICATE-----\n-----BEGIN CERTIFICATE-----\nMIIEkjCCA3qgAwIBAgIQCgFBQgAAAVOFc2oLheynCDANBgkqhkiG9w0BAQsFADA/\nMSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT\nDkRTVCBSb290IENBIFgzMB4XDTE2MDMxNzE2NDA0NloXDTIxMDMxNzE2NDA0Nlow\nSjELMAkGA1UEBhMCVVMxFjAUBgNVBAoTDUxldCdzIEVuY3J5cHQxIzAhBgNVBAMT\nGkxldCdzIEVuY3J5cHQgQXV0aG9yaXR5IFgzMIIBIjANBgkqhkiG9w0BAQEFAAOC\nAQ8AMIIBCgKCAQEAnNMM8FrlLke3cl03g7NoYzDq1zUmGSXhvb418XCSL7e4S0EF\nq6meNQhY7LEqxGiHC6PjdeTm86dicbp5gWAf15Gan/PQeGdxyGkOlZHP/uaZ6WA8\nSMx+yk13EiSdRxta67nsHjcAHJyse6cF6s5K671B5TaYucv9bTyWaN8jKkKQDIZ0\nZ8h/pZq4UmEUEz9l6YKHy9v6Dlb2honzhT+Xhq+w3Brvaw2VFn3EK6BlspkENnWA\na6xK8xuQSXgvopZPKiAlKQTGdMDQMc2PMTiVFrqoM7hD8bEfwzB/onkxEz0tNvjj\n/PIzark5McWvxI0NHWQWM6r6hCm21AvA2H3DkwIDAQABo4IBfTCCAXkwEgYDVR0T\nAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwfwYIKwYBBQUHAQEEczBxMDIG\nCCsGAQUFBzABhiZodHRwOi8vaXNyZy50cnVzdGlkLm9jc3AuaWRlbnRydXN0LmNv\nbTA7BggrBgEFBQcwAoYvaHR0cDovL2FwcHMuaWRlbnRydXN0LmNvbS9yb290cy9k\nc3Ryb290Y2F4My5wN2MwHwYDVR0jBBgwFoAUxKexpHsscfrb4UuQdf/EFWCFiRAw\nVAYDVR0gBE0wSzAIBgZngQwBAgEwPwYLKwYBBAGC3xMBAQEwMDAuBggrBgEFBQcC\nARYiaHR0cDovL2Nwcy5yb290LXgxLmxldHNlbmNyeXB0Lm9yZzA8BgNVHR8ENTAz\nMDGgL6AthitodHRwOi8vY3JsLmlkZW50cnVzdC5jb20vRFNUUk9PVENBWDNDUkwu\nY3JsMB0GA1UdDgQWBBSoSmpjBH3duubRObemRWXv86jsoTANBgkqhkiG9w0BAQsF\nAAOCAQEA3TPXEfNjWDjdGBX7CVW+dla5cEilaUcne8IkCJLxWh9KEik3JHRRHGJo\nuM2VcGfl96S8TihRzZvoroed6ti6WqEBmtzw3Wodatg+VyOeph4EYpr/1wXKtx8/\nwApIvJSwtmVi4MFU5aMqrSDE6ea73Mj2tcMyo5jMd6jmeWUHK8so/joWUoHOUgwu\nX4Po1QYz+3dszkDqMp4fklxBwXRsW10KXzPMTZ+sOPAveyxindmjkW8lGy+QsRlG\nPfZ+G6Z6h7mjem0Y+iWlkYcV4PIWL1iwBi8saCbGS5jN2p8M+X+Q7UNKEkROb3N6\nKOqkqm57TH2H3eDJAkSnh6/DNFu0Qg==\n-----END CERTIFICATE-----", "stdout_lines": ["-----BEGIN CERTIFICATE-----", "MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/", "MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT", "DkRTVCBSb290IENBIFgzMB4XDTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVow", "PzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1cmUgVHJ1c3QgQ28uMRcwFQYDVQQD", "Ew5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB", "AN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4O", "rz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEq", "OLl5CjH9UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9b", "xiqKqy69cK3FCxolkHRyxXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw", "7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40dutolucbY38EVAjqr2m7xPi71XAicPNaD", "aeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNV", "HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQMA0GCSqG", "SIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69", "ikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXr", "AvHRAosZy5Q6XkjEGB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZz", "R8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5", "JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubSfZGL+T0yjWW06XyxV3bqxbYo", "Ob8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ", "-----END CERTIFICATE-----", "-----BEGIN CERTIFICATE-----", "MIIEkjCCA3qgAwIBAgIQCgFBQgAAAVOFc2oLheynCDANBgkqhkiG9w0BAQsFADA/", "MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT", "DkRTVCBSb290IENBIFgzMB4XDTE2MDMxNzE2NDA0NloXDTIxMDMxNzE2NDA0Nlow", "SjELMAkGA1UEBhMCVVMxFjAUBgNVBAoTDUxldCdzIEVuY3J5cHQxIzAhBgNVBAMT", "GkxldCdzIEVuY3J5cHQgQXV0aG9yaXR5IFgzMIIBIjANBgkqhkiG9w0BAQEFAAOC", "AQ8AMIIBCgKCAQEAnNMM8FrlLke3cl03g7NoYzDq1zUmGSXhvb418XCSL7e4S0EF", "q6meNQhY7LEqxGiHC6PjdeTm86dicbp5gWAf15Gan/PQeGdxyGkOlZHP/uaZ6WA8", "SMx+yk13EiSdRxta67nsHjcAHJyse6cF6s5K671B5TaYucv9bTyWaN8jKkKQDIZ0", "Z8h/pZq4UmEUEz9l6YKHy9v6Dlb2honzhT+Xhq+w3Brvaw2VFn3EK6BlspkENnWA", "a6xK8xuQSXgvopZPKiAlKQTGdMDQMc2PMTiVFrqoM7hD8bEfwzB/onkxEz0tNvjj", "/PIzark5McWvxI0NHWQWM6r6hCm21AvA2H3DkwIDAQABo4IBfTCCAXkwEgYDVR0T", "AQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwfwYIKwYBBQUHAQEEczBxMDIG", "CCsGAQUFBzABhiZodHRwOi8vaXNyZy50cnVzdGlkLm9jc3AuaWRlbnRydXN0LmNv", "bTA7BggrBgEFBQcwAoYvaHR0cDovL2FwcHMuaWRlbnRydXN0LmNvbS9yb290cy9k", "c3Ryb290Y2F4My5wN2MwHwYDVR0jBBgwFoAUxKexpHsscfrb4UuQdf/EFWCFiRAw", "VAYDVR0gBE0wSzAIBgZngQwBAgEwPwYLKwYBBAGC3xMBAQEwMDAuBggrBgEFBQcC", "ARYiaHR0cDovL2Nwcy5yb290LXgxLmxldHNlbmNyeXB0Lm9yZzA8BgNVHR8ENTAz", "MDGgL6AthitodHRwOi8vY3JsLmlkZW50cnVzdC5jb20vRFNUUk9PVENBWDNDUkwu", "Y3JsMB0GA1UdDgQWBBSoSmpjBH3duubRObemRWXv86jsoTANBgkqhkiG9w0BAQsF", "AAOCAQEA3TPXEfNjWDjdGBX7CVW+dla5cEilaUcne8IkCJLxWh9KEik3JHRRHGJo", "uM2VcGfl96S8TihRzZvoroed6ti6WqEBmtzw3Wodatg+VyOeph4EYpr/1wXKtx8/", "wApIvJSwtmVi4MFU5aMqrSDE6ea73Mj2tcMyo5jMd6jmeWUHK8so/joWUoHOUgwu", "X4Po1QYz+3dszkDqMp4fklxBwXRsW10KXzPMTZ+sOPAveyxindmjkW8lGy+QsRlG", "PfZ+G6Z6h7mjem0Y+iWlkYcV4PIWL1iwBi8saCbGS5jN2p8M+X+Q7UNKEkROb3N6", "KOqkqm57TH2H3eDJAkSnh6/DNFu0Qg==", "-----END CERTIFICATE-----"]}

#22 - Oct 01, 2018 03:59 PM - Roberto Cirillo

- Status changed from Feedback to Closed

- % Done changed from 90 to 100

The CAFile with the root CA and the intermediate one, now is provided directly by playbook and not create on the fly.
I've tested it on mongo5-d-d4s.d4science.org and mongo1-d-d4s.d4science.org and it works properly. I'm going to close this ticket.