D4Science Infrastructure - Task #12450

Task # 12445 (Closed): SSL Certificate for mongodb development cluster

Manage SSL in the mongodb configuration template

Sep 10, 2018 04:22 PM - Andrea Dell'Amico

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, Production		

Description

Links to the documentation: https://docs.mongodb.com/v3.2/tutorial/configure-ssl/

Also the membership between cluster nodes can ben validated using certificates. See https://docs.mongodb.com/v3.2/tutorial/configure-x509-member-authentication/

History

#1 - Sep 11, 2018 04:56 PM - Andrea Dell'Amico

- Status changed from New to In Progress

- % Done changed from 0 to 30

I added some variables to the mongodb-org-3.2 role:

```
mongodb_ssl_enabled: False
mongodb_ssl_letsencrypt_managed: True
# Options: disabled, requireSSL, allowSSL, preferSSL
mongodb_ssl_mode: requireSSL
mongodb_ssl_certkey_file: /etc/pki/mongodb/mongodb.pem
mongodb_ssl_CA_file: /etc/ssl/certs/ca-certificates.crt
mongodb_ssl_allowConnectionsWithoutCertificates: 'true'
mongodb_ssl_disabled_protocols: 'TLS1_0,TLS1_1'
```

The corresponding configuration section, under net::

```
{% if mongodb_ssl_enabled %}
  ssl:
    mode: {{ mongodb_ssl_mode }}
    PEMKeyFile: '{{ mongodb_ssl_certkey_file }}'
    CAFile: '{{ mongodb_ssl_CA_file }}'
    disabledProtocols: {{ mongodb_ssl_disabled_protocols }}
    allowConnectionsWithoutCertificates: {{ mongodb_ssl_allowConnectionsWithoutCertificates }}
{% endif %}
```

The configuration for the d4science cluster should be, initially:

```
  ssl:
    mode: preferSSL
    PEMKeyFile: /etc/pki/mongodb/mongodb.pem
    CAFile: /etc/ssl/certs/ca-certificates.crt
    disabledProtocols: TLS1_0,TLS1_1
    allowConnectionsWithoutCertificates: true
```

The /etc/pki/mongodb/mongodb.pem file will be put in place by a letsencrypt hook script.

preferSSL should be changed to requireSSL after we've verified that all the client applications connect over SSL correctly.

allowConnectionsWithoutCertificates can be set to false if we want to verify the clients certificates: in that case, the clients must be configured to present their certificate.

#2 - Sep 11, 2018 05:12 PM - Andrea Dell'Amico

- Status changed from In Progress to Closed

- % Done changed from 30 to 100

#3 - Sep 11, 2018 05:13 PM - Andrea Dell'Amico

We do not have a completely managed cluster, so I didn't touch the configuration that provides x509 authentication between cluster members.