OpenNebula - Feature #5257
Explain how to add HTTPS to XMLRPC

07/20/2017 08:53 AM - OpenNebula Systems Support Team

Status:	New	**Start date:**	07/20/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Documentation	**Estimated time:**	0.00 hour
Target version:	Release 5.4.4		
Resolution:		**Pull request:**	

Description

To harden OpenNebula based clouds. Using an SSL proxy like nginx

History

#1 - 07/20/2017 09:44 AM - OpenNebula Systems Support Team

Notes for the docs:

```
$ cat /etc/nginx/conf.d/opennebula-ssl.conf
server {
    listen 2634 ssl;
    ssl_certificate         /etc/nginx/nginx.crt;
    ssl_certificate_key     /etc/nginx/nginx.key;
    location / {
        proxy_pass          http://localhost:2633;
    }
}
```

```
export ONE_XMLRPC=https://localhost:2634/RPC2
or one_endpoint
```

```
export ONE_DISABLE_SSL_VERIFY=true
```

#2 - 07/24/2017 10:04 AM - Ruben S. Montero

- Target version changed from Release 5.6 to Release 5.4.1

#3 - 08/14/2017 09:02 AM - Strahinja Kustudic

I'm willing to write this documentation, but I'm not sure where exactly to add it. I was thinking to add it to frontend_installation.rst similar like MySQL is added as option and than make a separate page about it, but I'm not sure if that is the best way to do it?

#4 - 09/11/2017 06:24 PM - Kristian Feldsam

Hii all, I like to share my config. I also use limit_req_zone to limit max connections to api

```
# main server config /etc/nginx/nginx.conf
# For more information on configuration, see:
#   * Official English Documentation: http://nginx.org/en/docs/
#   * Official Russian Documentation: http://nginx.org/ru/docs/

user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

events {
    worker_connections 1024;
}

http {
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile            on;
    tcp_nopush          on;
    tcp_nodelay         on;
    keepalive_timeout   65;
    types_hash_max_size 2048;
    server_names_hash_bucket_size 64;

    include             /etc/nginx/mime.types;
    default_type        application/octet-stream;

    client_max_body_size 20M;

    limit_req_zone $binary_remote_addr zone=perip:10m rate=24r/s; # one tenth of MAX_CONN from oned.conf
    limit_req_zone $server_name zone=perserver:10m rate=240r/s; # MAX_CONN from oned.conf

    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # See http://nginx.org/en/docs/ngx_core_module.html#include
    # for more information.
    include /etc/nginx/conf.d/*.conf;
}

# vhost config in /etc/nginx/conf.d/
server {
    listen 443;
    server_name  cloud-api.domain.tld;

    ssl on;
     ssl_certificate /etc/nginx/nginx.crt;
     ssl_certificate_key /etc/nginx/nginx.key;
     ssl_session_timeout 1d;
     ssl_session_cache shared:SSL:50m;
```

```
        # Diffie-Hellman parameter for DHE ciphersuites, recommended 2048 bits
         ssl_dhparam /etc/nginx/dhparams.pem;

        # intermediate configuration. tweak to your needs.
         ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
         ssl_ciphers
    'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1
    HA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256
    SA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256';
         ssl_prefer_server_ciphers on;

        # HSTS (ngx_http_headers_module is required) (15768000 seconds = 6 months)
         add_header Strict-Transport-Security max-age=15768000;

        # Load configuration files for the default server block.
        include /etc/nginx/default.d/*.conf;

        location / {
            limit_req zone=perip burst=48; # one tenth of MAX_CONN_BACKLOG from oned.conf
            limit_req zone=perserver burst=480;  #  MAX_CONN_BACKLOG from oned.conf

            proxy_set_header   Host             $host;
            proxy_set_header   X-Real-IP        $remote_addr;
            proxy_set_header   X-Forwarded-For  $proxy_add_x_forwarded_for;
            proxy_pass http://127.0.0.1:2633;
        }
    }
```

#5 - 09/21/2017 01:48 PM - kvaps kvaps

This is how to connect to opennebula remotely:

```
sudo gem install --no-user-install  opennebula-cli
echo "export ONE_XMLRPC=https://opennebula-backend.tld/RPC2" >> .bashrc
echo "export ONE_DISABLE_SSL_VERIFY=true" >> .bashrc
```

After re login to bash:

```
mkdir .one
touch .one/one_auth
oneuser login myuser
```

#6 - 10/11/2017 02:14 PM - Ruben S. Montero

- Target version changed from Release 5.4.1 to Release 5.4.3

#7 - 11/15/2017 04:32 PM - OpenNebula Systems Support Team

- Target version changed from Release 5.4.3 to Release 5.4.4