uts-server - RFC 3161 Timestamp Server

Release 0.0.1

September 11, 2016

Contents

CHAPTER 1

Dependencies

1.1 Runtime dependencies

List of dependencies uts-server relies on to run:

- OpenSSL.
- civetweb.

1.2 Build dependencies

List of dependencies needed to build civetweb:

- cmake
- either gcc or clang

CHAPTER 2

Compilation

uts-server is compiled using cmake:

```
# If civetweb is already present on the system
$ cmake .
$ make

# If civetweb is not present
# this will get the proper tag of civetweb from upstream and compile it
$ cmake . -DBUNDLE_CIVETWEB=ON
$ make

# Compile with debug flags
$ cmake . -DDEBUG=ON
$ make
```

CHAPTER 3

Configuration Parameters

3.1 Section [main]

Main configuration section (mostly http configuration).

Parameter	Description	Example Value
access_control_allow_origin	Comma separated list of IP subnets to accept/deny Ex: -0.0.0.0/0,+192.168.0.0/16 (deny all accesses, only allow 192.168.0.0/16 subnet)	-0.0.0.0/0,+192.168/16
enable_keep_alive	Allows clients to reuse TCP connection for subsequent HTTP requests, which improves performance.	no
listening_ports	Comma-separated list of IP:port tuples to listen on. If the port is SSL, a letter s must be appended. Ex: listening_ports = 80,443s	127.0.0.1:2020
log_level	Loglevel (debug, info, notice, warn, err, emerg, crit)	info
num_threads	Number of worker threads.	50
request_timeout_ms	Timeout for network read and network write operations. In milliseconds.	30000
run_as_user	Switch to given user credentials after startup. Required to run on privileged ports as non root user.	uts-server
ssl_ca_file	Path to a .pem file containing trusted certificates. The file may contain more than one certificate.	/etc/uts-server/ca.pem
ssl_ca_path	Name of a directory containing trusted CA certificates.	/etc/ssl/ca/
ssl_certificate	Path to the SSL certificate file . PEM format must contain private key and certificate.	/etc/uts-server/cert.pem
ssl_cipher_list	See https://www.openssl.org/docs/manmaster/apps/ciphers.html for more detailed	ALL:!eNULL
ssl_default_verify_paths	Loads default trusted certificates locations set at OpenSSL compile time.	yes
ssl_protocol_version	Sets the minimal accepted version of SSL/TLS protocol according to the table: • SSL2+SSL3+TLS1.0+TLS1.1+TLS1.2 -> 0 • SSL3+TLS1.0+TLS1.1+TLS1.2 -> 1 • TLS1.0+TLS1.1+TLS1.2 -> 2 • TLS1.1+TLS1.2 -> 3 • TLS1.2 -> 4	3
ssl_short_trust	Enables the use of short lived certificates	no
ssl_verify_depth	Sets maximum depth of certificate chain. If client's certificate chain is longer than the depth set here connection is refused.	9
ssl_verify_peer	Enable client's certificate verification by the server.	yes
tcp_nodelay	Enable TCP_NODELAY socket option on client connections.	0
throttle	Limit download speed for clients. Throttle is a comma-separated list of key=value pairs;	*=0

3.2 Section [oids]

Section for declaring OID mapping. Just add <name> = <OID> pairs.

Parameter	Description	Example Value
tsa_policy1		1.2.3.4.1
tsa_policy2		1.2.3.4.5.6
tsa_policy3		1.2.3.4.5.7

3.3 Section [tsa]

Section defining which TSA section to use.

Parameter	Description	Example Value
default_tsa	Name of the TSA section to use as default.	tsa_config1

3.4 Section [tsa_config1]

Example of Time-Stamp section configuration.

Parameter	Description	Example Value
accuracy	Time-Stamp accuracy. (optional)	secs:1, millisecs:500, microsecs:100
certs	Certificate chain to include in reply. (optional)	$dir/cacert.pem
clock_precision_digits	Number of decimals for Time-Stamp. (optional)	0
crypto_device	OpenSSL engine to use for signing.	builtin
default_policy	Policy if request did not specify it. (optional)	tsa_policy1
digests	Acceptable message digests. (mandatory)	md5, sha1
dir	TSA root directory.	/etc/uts-server/pki
ess_cert_id_chain	Must the ESS cert id chain be included? (optional, default: no)	no
ordering	Is ordering defined for timestamps? (optional, default: no)	yes
other_policies	Acceptable policies. (optional)	tsa_policy2, tsa_policy3
signer_cert	The TSA signing certificat. (optional)	$dir/tsacert.pem
signer_key	The TSA private key. (optional)	$dir/private/tsakey.pem
tsa_name	Must the TSA name be included in the reply? (optional, default: no)	yes

CHAPTER 4

Full Configuration File

```
# Section for declaring OID mapping. Just add <name> = <OID> pairs.
[ oids ]

tsa_policy1 = 1.2.3.4.1
tsa_policy2 = 1.2.3.4.5.6
tsa_policy3 = 1.2.3.4.5.7

# Main configuration section (mostly http configuration).
[ main ]

# Comma-separated list of IP:port tuples to listen on.
# If the port is SSL, a letter s must be appended.
#
# Ex: listening_ports = 80,443s
listening_ports = 127.0.0.1:2020

# Allows clients to reuse TCP connection for subsequent
# HTTP requests, which improves performance.
enable_keep_alive = no

# Number of worker threads.
num_threads = 50

# Switch to given user credentials after startup.
# Required to run on privileged ports as non root user.
#run_as_user = uts-server

# Limit download speed for clients.
#
# Throttle is a comma-separated list of key=value pairs:
#
# - *            -> limit speed for all connections
#
# - x.x.x.x/mask ->  limit speed for specified subnet
#
# The value is a floating-point number of bytes per second,
# optionally followed by a k or m character
# meaning kilobytes and megabytes respectively.
#
# A limit of 0 means unlimited rate.
#
# Ex: throttle = *=1k,10.10.0.0/16=10m,10.20.0.0/16=0
throttle = *=0
```

```
# Timeout for network read and network write operations.
# In milliseconds.
request_timeout_ms = 30000

# Path to the SSL certificate file .
# PEM format must contain private key and certificate.
#ssl_certificate = /etc/uts-server/cert.pem

# Enable client's certificate verification by the server.
#ssl_verify_peer = yes

# Name of a directory containing trusted CA certificates.
#ssl_ca_path = /etc/ssl/ca/

# Path to a .pem file containing trusted certificates.
# The file may contain more than one certificate.
#ssl_ca_file = /etc/uts-server/ca.pem

# Sets maximum depth of certificate chain.
# If client's certificate chain is longer
# than the depth set here connection is refused.
#ssl_verify_depth = 9

# Loads default trusted certificates
# locations set at OpenSSL compile time.
#ssl_default_verify_paths = yes

# See https://www.openssl.org/docs/manmaster/apps/ciphers.html
# for more detailed
#ssl_cipher_list = ALL:!eNULL

# Sets the minimal accepted version of SSL/TLS protocol
# according to the table:
#
# - SSL2+SSL3+TLS1.0+TLS1.1+TLS1.2 -> 0
#
# - SSL3+TLS1.0+TLS1.1+TLS1.2      -> 1
#
# - TLS1.0+TLS1.1+TLS1.2           -> 2
#
# - TLS1.1+TLS1.2                  -> 3
#
# - TLS1.2                         -> 4
#ssl_protocol_version = 3

# Enables the use of short lived certificates
#ssl_short_trust = no

# Comma separated list of IP subnets to accept/deny
#
# Ex: -0.0.0.0/0,+192.168.0.0/16
# (deny all accesses, only allow 192.168.0.0/16 subnet)
#access_control_allow_origin = -0.0.0.0/0,+192.168/16

# Enable TCP_NODELAY socket option on client connections.
tcp_nodelay = 0

# Loglevel (debug, info, notice, warn, err, emerg, crit)
```

```
log_level = info

# Section defining which TSA section to use.
[ tsa ]

# Name of the TSA section to use as default.
default_tsa = tsa_config1

# Example of Time-Stamp section configuration.
[ tsa_config1 ]

# TSA root directory.
dir = /etc/uts-server/pki

# OpenSSL engine to use for signing.
#crypto_device        = builtin

# The TSA signing certificat. (optional)
signer_cert = $dir/tsacert.pem

# Certificate chain to include in reply. (optional)
certs = $dir/cacert.pem

# The TSA private key. (optional)
signer_key = $dir/private/tsakey.pem

# Policy if request did not specify it. (optional)
default_policy = tsa_policy1

# Acceptable policies. (optional)
other_policies = tsa_policy2, tsa_policy3

# Acceptable message digests. (mandatory)
digests = md5, sha1

# Time-Stamp accuracy. (optional)
accuracy = secs:1, millisecs:500, microsecs:100

# Number of decimals for Time-Stamp. (optional)
clock_precision_digits = 0

# Is ordering defined for timestamps? (optional, default: no)
ordering = yes

# Must the TSA name be included in the reply? (optional, default: no)
tsa_name = yes

# Must the ESS cert id chain be included? (optional, default: no)
ess_cert_id_chain = no
```

CHAPTER 5

Deploy

5.1 Usage

```
$ ./uts-server --help
Usage: uts-server [OPTION...] -c CONFFILE [-d] [-D] [-p <pidfile>]

UTS micro timestamp server (RFC 3161)

  -c, --conffile=CONFFILE    Path to configuration file
  -d, --daemonize            Launch as a daemon
  -D, --debug                STDOUT debugging
  -p, --pidfile=PIDFILE      Path to pid file
  -?, --help                 Give this help list
      --usage                Give a short usage message
  -V, --version              Print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.

Report bugs to Pierre-Francois Carpentier <carpentier.pf@gmail.com>.
```

5.2 Running uts-sever

To debug problems with uts-server, run it in the foreground in debug mode:

```
# In debug mode with verbose debugging on stdout
$ ./uts-server -c <path/to/conf> -D
```

To run it as a daemon:

```
# In daemon mode
$ ./uts-server -c <path/to/conf> -d -p <path/to/pidfile>
```

CHAPTER 6

Changelogs

6.1 dev

CHAPTER 7

uts-server

Micro RFC 3161 Time-Stamp server written in C.

Doc Uts-Server documentation on ReadTheDoc

Dev Uts-Server source code on GitHub

Author Pierre-Francois Carpentier - copyright © 2016

7.1 Status

Alpha

7.2 License

7.3 Quick Start

```
# Building with civetweb embedded (will recover civetweb from github).
$ cmake . -DBUNDLE_CIVETWEB=ON
$ make

# Create some test certificates.
$ ./tests/cfg/pki/create_tsa_certs

# Launching the time-stamp server with test configuration in debug mode.
$ ./uts-server -c tests/cfg/uts-server.cnf -D

# In another shell, launching a time-stamp script on the README.md file.
```

```
$ ./goodies/timestamp-file.sh -i README.rst -u http://localhost:2020 -r -O "-cert";

# Verify the time-stamp.
$ openssl ts -verify -in README.rst.tsr -data README.rst -CAfile ./tests/cfg/pki/tsaca.pem

# Display the time-stamp content.
$ openssl ts -reply -in README.rst.tsr -text
```

7.4 Powered by