ConfD FIPS Mode Support

Wai Tai
Solutions Architect
October 22, 2019

Topics

- FIPS background
- OpenSSL
- FIPS mode in ConfD
- Demo

What is FIPS?

- FIPS are standards specified by the US Government for approving cryptographic software
- FIPS 140-2 standards are usually required to sell into the U.S. government

OpenSSL

- provides support for TLS and SSL protocols
- is a general-purpose cryptography library
- ConfD depends on the OpenSSL libcrypto shared library for its cryptographic functions

FIPS Object Module

- is an optional component embedded in OpenSSL
- provides an API for invocation of only FIPS approved cryptographic functions from OpenSSL
- It is the FOM and not the OpenSSL library that gets FIPS validated

FIPS Capable OpenSSL

- Both the FOM and OpenSSL library are separately built with the FOM embedded within the OpenSSL library as part of the OpenSSL build process
- The ”fips” configuration option needs to be specified when building OpenSSL
- The FIPS Capable OpenSSL attempts to disable non-FIPS algorithms when FIPS mode is enabled
  - The disabling occurs on the EVP_* APIs and most low level function calls
    - Responsibility of application developers to not use non-FIPS algorithms

How do you install FIPS Capable OpenSSL?

- OpenSSL 1.0.2
  - Build from source
    - https://wiki.openssl.org/index.php/FIPS_Library_and_Apache
  - First build the FOM
    - Latest version is 2.0.12
    - By default, the built FOM will be at /usr/local/ssl/fips-2.0/lib
  - Then build the OpenSSL library
    - Latest version is 1.0.2t
    - ./config fips shared --prefix=/usr/local/ssl --openssldir=/usr/local/ssl
  - Modify LD_LIBRARY_PATH to use the FIPS capable OpenSSL library (/usr/local/ssl/lib)
  - Run the FIPS capable OpenSSL at /usr/local/ssl/bin/openssl

ConfD’s support of FIPS mode

- The version of Erlang OTP being used by previous versions of ConfD didn’t support FIPS mode
  - The Erlang crypto module invokes only low level OpenSSL library calls
- With the recent upgrade to Erlang OTP 20, FIPS mode support can now be enabled starting with 7.2

ConfD's support of libcrypto

- ConfD's Linux distributions are built with OpenSSL 1.0.0 and thus require libcrypto.so.1.0.0
- Two ConfD components have libcrypto dependency
  - libconfd library used by ConfD client applications
  - crypto.so used by the ConfD daemon as an interface to libcrypto
  - Source code is provided for these two components to be rebuilt with a different OpenSSL version with or without fips support

How to rebuild crypto.so?

- Untar the confd-<vsn>.libconfd.tar.gz tar archive from your ConfD distribution
- Follow the instructions in the top level README file included in the tar archive
  - make FIPS_LIBCRYPTO=yes USE_SSL_DIR=/usr/local/ssl crypto
  - make install_crypto
    - confdrc needs to be sourced first

How to rebuild libconfd.so?

- Untar the confd-<vsn>.libconfd.tar.gz tar archive from your ConfD distribution
- Follow the instructions in the top level README file included in the tar archive
  - make USE_SSL_DIR=/usr/local/ssl
  - make install
    - confdrc needs to be sourced first
  - Use ConfD 7.2.1 or later releases

How to enable FIPS mode in ConfD?

- confd.conf

```
<fipsMode>
  <enabled>true</enabled>
</fipsMode>
```

FIPS Compliant algorithms & crypto suites

- confd.conf parameters to configure
  - /confdConfig/cryptHash/algorithm – no md5, use sha-256 or sha-512
  - /confdConfig/ssh/algorithms – kex, mac, and encryption
    - FIPS doesn't support the mac algorithms of hmac-md5 & hmac-md5-96
  - /confdConfig/webui/transport/ssl/ciphers
  - /confdConfig/webui/transport/ssl/ellipticCurves

Demo