ubuntu

Canonical FIPS 140-2 Certified Modules

Federal Information Processing Standards Publications (FIPS) are issued by the National Institute of Standards and Technology (NIST). FIPS 140-2 specifies the security requirements for cryptographic modules. These requirements address the areas of secure design and implementation.

Certification information

Canonical has certified several of Ubuntu's cryptographic modules at Level 1.

Releases
Ubuntu 16.04 LTS

Architectures Certified
amd64
ppc64el
s390x

Platform Models Certified
IBM Power System S822L (PowerNV 8247-22L)
IBM Power System S822LC (PowerNV 8001-22C)
IBM Power System S822LC (PowerNV 8335-GTB)
Supermicro SYS-5018R-WR
IBM z13 (running on LPAR)

Modules Certified
Kernel Crypto API
NIST Kernel Crypto Security Policy
OpenSSL
NIST OpenSSL Security Policy
OpenSSH Client
NIST OpenSSH Client Security Policy
OpenSSH Server
NIST OpenSSH Server Security Policy
Strongswan
NIST Strongswan Security Policy

Obtaining Canonical's FIPS 140-2 Certified Modules

Canonical's FIPS 140-2 Certified Modules are available to customers who have purchased qualifying Ubuntu Advantage products. The modules are available as packages in a private Launchpad PPA. Each package in the PPA is signed with a unique PGP key to ensure authenticity.

To access the FIPS packages you will need to request access to the FIPS PPA from Canonical. You will be notified once your access has been granted, after which you can obtain your PPA credentials from Launchpad as follows:

Once you have verified your access to the Launchpad FIPS PPA, as follows:

1. Click this link to view your Private PPA subscriptions
2. Under Archive locate the FIPS (ppa:ubuntu-advantage/fips) line and click View on the right
3. Locate the line starting with "deb https://<your-launchpad-id>:<PPA-password>@", where "<your-launchpad-id>:<PPA-password>" represent your personal Launchpad username and the encoded password created for this PPA.
4. Select and copy the portion comprising of <your-launchpad-id>:<PPA-password>.

Installing FIPS 140-2 Certified Modules

There are two methods for installing the FIPS 140-2 Certified Modules on Ubuntu 16.04 LTS. The modules can be installed using the ubuntu-advantage-tools package available from the Ubuntu Repositories or they can be manually installed and configured.

AUTOMATED INSTALLATION

1. Ensure that the ubuntu-advantage-tools package is up to date

   ```
   sudo apt update && sudo apt install ubuntu-advantage-tools
   ```

2. Enable FIPS via the ubuntu-advantage script

   ```
   sudo ubuntu-advantage enable-fips <your-launchpad-id>:<PPA-password>
   ```

3. Upon successfully updating the bootloader, the system is now ready to be rebooted. You MUST reboot to put the system into FIPS mode. The reboot will boot into the FIPS-supported kernel and create the /proc/sys/crypto/fips_enabled entry which tells the FIPS certified modules to run in FIPS mode. If you fail to reboot after installing and configuring the bootloader, the certified modules will NOT run in FIPS mode.

4. To verify that FIPS is enabled after the reboot:

   a. Check the /proc/sys/crypto/fips_enabled file and ensure it is set to 1.

   b. If it is set to 0, the FIPS modules will not run in FIPS mode.

5. Proceed to the Caution section of the document.

MANUAL INSTALLATION

Setting up the FIPS repository

1. Add the unique PPA PGP key onto the system.

   ```
   sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 8D13028C
   ```

2. Add the FIPS PPA repository to the system that the FIPS 140-2 Certified Modules will be installed on. The following command is a single line.

   ```
   sudo add-apt-repository -u 'deb
   https://<your-launchpad-id>:<PPA-password>@private-ppa.launchpad.net/ubuntu-advantage/fips/ubuntu xenial main'
   ```

Install the packages

Install the certified modules along with the corresponding HMAC packages. Please note, if you do not install the separate HMAC packages, the modules will fail to be configured in FIPS mode. The HMAC packages contain a hash for each module. This hash allows the module to perform the FIPS 140-2 requirement of integrity checking at startup. If a module fails to check its integrity, it will not run in FIPS mode.

```
sudo apt install openssh-client openssh-client-hmac openssh-server
openssh-server-hmac openssl libssl1.0.0 libssl1.0.0-hmac fips-initramfs linux-fips
strongswan strongswan-hmac
```

Note: The linux-fips package includes the Kernel Crypto API HMAC package.

Continued…

Configure FIPS mode

Upon successful installation of the certified modules and HMAC packages, the system needs to be configured to instruct the modules to run in FIPS mode.

- If the system has a separate boot partition, proceed to Separate boot partition
- If the system does not have a separate boot partition, proceed to either of the following sections:

  Configure ppc64el and amd64 architectures
  Configure s390x architecture

Separate boot partition

View /etc/fstab and find the entry containing "/boot" and the associated UUID. Note the UUID as it will be needed later.

An example /etc/fstab, with the "/boot" entry highlighted:

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>        <dump>     <pass>
# / was on /dev/vda3 during installation
UUID=3eabf0c6-f4a2-4212-8b3e-7918bbcabfcf /               ext4       errors=remount-ro  0   1
# /boot was on /dev/vda1 during installation
UUID=96e8fdc4-c03b-4a34-b5ee-1e5a1cac9e8c /boot           ext2       defaults           0   2
# swap was on /dev/vda5 during installation
UUID=a0de8f81-5750-4ade-8a8b-64b6441cddf0 none            swap       sw                 0   0
```

Depending on the system's architecture, proceed to either of the following sections:

Configure ppc64el and amd64 architectures
Configure s390x architecture

Continued…

Configure ppc64el and amd64 architectures

Configure GRUB

Configure the GRUB bootloader to use FIPS by default.

1. Create the directory "/etc/default/grub.d", if it does not already exist.

   ```
   mkdir /etc/default/grub.d
   ```

2. Switch to the directory.

   ```
   cd /etc/default/grub.d
   ```

3. Create and edit a file named "99-fips.cfg".

   ```
   vi 99-fips.cfg
   ```

4. Depending on your configuration, you will choose one of the options below to place in "99-fips.cfg".

   a. Without a separate boot partition.
   ```
   GRUB_CMDLINE_LINUX_DEFAULT="$GRUB_CMDLINE_LINUX_DEFAULT fips=1"
   ```

   b. With a separate boot partition, place the boot UUID that was noted earlier in the highlighted section.
   ```
   GRUB_CMDLINE_LINUX_DEFAULT="$GRUB_CMDLINE_LINUX_DEFAULT fips=1 bootdev=UUID=Insert boot UUID"
   ```

5. Proceed to the Update GRUB section

Update GRUB

Update the bootloader with the new configuration.

1. Run the following command to update the GRUB boot configuration

   ```
   sudo update-grub
   ```

2. Proceed to the Reboot section.

Continued…

Configure s390x architecture

Configure Zipl

Configure the Zipl bootloader to use FIPS by default.

1. Edit /etc/zipl.conf, and add “fips=1”. Example:

```
[ubuntu]
target = /boot
image = /boot/vmlinuz
ramdisk = /boot/initrd.img
parameters = root=UUID=dfd315ca-c76c-4a76-9e3f-462cb919c572 crashkernel=196M fips=1
```

2. If the system has a separate boot partition, the boot UUID must be added to the “parameters” line for the FIPS kernel. The example below has the “parameters” line wrapped.

```
[ubuntu]
target = /boot
image = /boot/vmlinuz
ramdisk = /boot/initrd.img
parameters = root=UUID=dfd315ca-c76c-4a76-9e3f-462cb919c572 crashkernel=196M
fips=1 bootdev=UUID=Insert Boot UUID
```

3. Proceed to the Update Zipl section.

Update Zipl

Update the bootloader with the new configuration.

1. Run the following command to update Zipl.

```
sudo zipl
```

2. Proceed to the Reboot section.

Continued…

Reboot

Upon successfully updating the bootloader, the system is now ready to be rebooted. You MUST reboot to put the system into FIPS mode. The reboot will boot into the FIPS-supported kernel and create the /proc/sys/crypto/fips_enabled entry which tells the FIPS certified modules to run in FIPS mode. If you fail to reboot after installing and configuring the bootloader, the certified modules will NOT run in FIPS mode.

To verify that FIPS is enabled after the reboot:

1. Check the /proc/sys/crypto/fips_enabled file and ensure it is set to 1.
   a. If it is set to 0, the FIPS modules will not run in FIPS mode.

Caution

A manual update to a FIPS certified package will cause the FIPS certified module to be overwritten. It is recommended to not update the FIPS certified packages to prevent overwriting them.

To prevent the FIPS 140-2 Certified Modules from being overwritten on a system update, it is recommended to put a hold on the FIPS certified packages.

For example:

```
sudo apt-mark hold openssh-client openssh-client-hmac
```