目 录

1 FIPS

1.1 FIPS配置命令

1.1.1 display fips status

display fips status 命令用来显示 FIPS 模式状态。

【命令】

display fips status

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【举例】

显示 FIPS 模式状态。

```
<Sysname> display fips status
FIPS mode is enabled.
```

【相关命令】

- **fips mode enable**

1.1.2 fips mode enable

fips mode enable 命令用来开启 FIPS 模式。

undo fips mode enable 命令用来关闭 FIPS 模式。

【命令】

fips mode enable

undo fips mode enable

【缺省情况】

FIPS 模式处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

开启 FIPS 模式并重启设备之后，设备会运行于支持 FIPS 140-2 标准的工作模式下。在该工作模式下，系统将具有更为严格的安全性要求，并会对密码模块进行相应的自检处理，以确认其处于正常运行状态。

用户执行了 **fips mode enable** 命令后，系统提供以下两种启动方式来进入 FIPS 模式：

- 自动重启方式：

  该方式下，系统自动创建一个 FIPS 缺省配置文件（名称为 fips-startup.cfg），同时将其指定为下次启动配置文件，并且要求用户手工配置设备重启后登录设备的用户名和密码。如果用户在输入过程中想退出配置流程，可以使用<Ctrl+C>组合键中断配置流程，配置流程中断后，当前的 **fips mode enable** 命令设置也相应失败。

  用户成功设置安全管理员用户名和登录密码之后，系统将自动使用指定的启动配置文件重启。

- 手动重启方式：

  该方式下，系统不自动创建进入 FIPS 模式的下次启动配置文件。需要用户手工完成进入 FIPS 模式所需的所有必要配置，主要包括：

  - 开启全局 Password Control 功能。
  - 设置全局 Password Control 密码组合类型的个数为 4，每种类型至少 1 个字符。
  - 设置全局 Password Control 的密码最小长度为 15。
  - 添加设备管理类本地用户，设置密码、用户角色和服务类型。本地用户的密码需要符合以上 Password Control 配置的限制，用户角色必须是 network-admin 或者 mdc-admin，服务类型为 terminal。
  - 删除不符合 FIPS 标准的本地用户服务类型（Telnet、HTTP 和 FTP）。

  然后手工保存当前配置文件为下次启动配置文件，并将二进制类型的下次启动配置文件删除后重启设备。

执行 **fips mode enable** 命令之后，系统会提示用户选择启动方式，若用户未在 30 秒内作出选择，则系统默认用户采用了手动启动方式。

用户执行了 **undo fips mode enable** 命令后，系统提供以下两种启动选择来退出 FIPS 模式：

- 自动重启方式：系统自动创建一个非 FIPS 缺省配置文件（名称为 non-fips-startup.cfg），同时将其指定为下次启动配置文件，之后自动使用非 FIPS 缺省配置文件重启。重启之后，当前登录用户不需要输入任何信息即可直接登录到非 FIPS 模式的系统。
- 手动重启方式：系统不自动创建进入非 FIPS 模式的下次启动配置文件，需要用户手工完成进入非 FIPS 模式所需的所有必要配置之后，手工重启设备。重启之后，当前登录用户需要根据配置的登录认证方式输入相应的用户信息登录到非 FIPS 模式的系统。

【举例】

开启 FIPS 模式，并选择自动重启方式进入 FIPS 模式。

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:y
The system will create a new startup configuration file for FIPS mode. After you set the login username and password for FIPS mode, the device will reboot automatically.
Enter username(1-55 characters): root
```

```
Enter password(15-63 characters):
Confirm password:
Waiting for reboot... After reboot, the device will enter FIPS mode.
```

开启 FIPS 模式，并选择手动重启方式进入 FIPS 模式。

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:n
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.
```

关闭 FIPS 模式，并选择自动重启方式进入非 FIPS 模式。

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode and then reboot
automatically. Continue? [Y/N]:y
Waiting for reboot... After reboot, the device will enter non-FIPS mode.
```

关闭 FIPS 模式，并选择手动重启方式进入非 FIPS 模式。

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode, and then reboot
automatically. Continue? [Y/N]:n
Change the configuration to meet non-FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter non-FIPS mode.
```

【相关命令】

- **display fips status**

1.1.3 fips self-test

fips self-test 命令用来手工触发密码算法自检。

【命令】

fips self-test

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

当管理员需要确认当前处于 FIPS 模式的系统中的密码算法模块是否正常工作时，可以执行本命令触发密码算法自检。手工触发的密码算法自检内容与设备启动时自动进行的启动自检内容相同。

只有所有密码算法自检都通过了，整个密码算法自检才算成功。密码算法自检失败后，设备会自动重启。

【举例】

手工触发密码算法自检。

```
<Sysname> system-view
[Sysname] fips self-test
Cryptographic Algorithms Known-Answer Tests are running ...

CPU 0 of slot 0 in chassis 0:
Starting Known-Answer tests in the user space.
Known-answer test for SHA1 passed.
Known-answer test for SHA224 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA224 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for AES passed.
Known-answer test for RSA(signature/verification) passed.
Known-answer test for RSA(encrypt/decrypt) passed.
Known-answer test for DSA(signature/verification) passed.
Known-answer test for random number generator passed.
Known-Answer tests in the user space passed.
Starting Known-Answer tests in the kernel.
Known-answer test for AES passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for SHA1 passed.
Known-answer test for GCM passed.
Known-answer test for GMAC passed.
Known-answer test for random number generator passed.
Known-Answer tests in the kernel passed.

CPU 0 of slot 1 in chassis 0:
Starting Known-Answer tests in the user space.
Known-answer test for SHA1 passed.
Known-answer test for SHA224 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA224 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for AES passed.
Known-answer test for RSA(signature/verification) passed.
Known-answer test for RSA(encrypt/decrypt) passed.
Known-answer test for DSA(signature/verification) passed.
Known-answer test for random number generator passed.
```

```
Known-Answer tests in the user space passed.
Starting Known-Answer tests in the kernel.
Known-answer test for AES passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for SHA1 passed.
Known-answer test for GCM passed.
Known-answer test for GMAC passed.
Known-answer test for random number generator passed.
Known-Answer tests in the kernel passed.
Cryptographic Algorithms Known-Answer Tests passed.
```