自定义改密脚本配置举例

目 录

1 自定义改密脚本概述

针对常见的目标设备类型，运维审计系统有默认的接近 40 种改密方式。

但是仍然会有目标设备不符合这 40 种的改密方式，所以需要自定义改密脚本。

自定义改密脚本仅支持 TUI 会话。

2 自定义改密脚本配置

自定义改密需要提前准备好改密命令交互过程。

例如：

[root@101 ~]# passwd xhf

Changing password for user xhf.

New password:

BAD PASSWORD: The password is shorter than 8 characters

Retype new password:

passwd: all authentication tokens updated successfully.

网络设备改密

<H3C>system-view

Enter system view, return user view with Ctrl+Z.

[H3C]aaa

[H3C-aaa]local-user h3c password cipher XXXXXXX

[H3C-aaa]quit

[H3C]quit

<H3C>save

The current configuration will be written to the device.

Are you sure to continue?[Y/N]y

Now saving the current configuration to the slot 0.

2.1 改密方式界面介绍

(1) 进入超级管理员账户。

(2) 进入“策略配置”-“改密方式”菜单。点击“添加”。

图2-1 改密方式路径

图2-2 改密方式界面

参数说明：

- 名称：改密脚本的名称。
- 特权改密：勾选则通过特权账号进行改密。不勾选则通过改密账号进行改密。
- 简要说明：描述该改密脚本。
- 系统账号：针对指定的系统账号进行以下步骤的改密过程。留空是针对所有系统账号进行以下步骤的改密过程。
- stepN：代表进行改密过程的交互式操作。
- 增加新步骤：增加 stepN。
- 删除配置：删除该系统账号下的所有步骤。
- 增加账号配置：增加一个新账号以及其步骤。
- 标题说明：
  - **expect**：等待输出匹配内容；如果匹配，就输出对应 send 的内容。当匹配的内容有多行时，只匹配最后一行的内容
  - **send**：匹配后发送的命令；执行完此命令，会进行下一个 expect 的匹配。

- **error_expect：**等待错误输出时的匹配；当改密过程有错误输出，导致改密不成功，可以在这里匹配，匹配后，会终止改密过程。
- **error_report：**自定义错误报告；当匹配 error_expect，改密停止时，可以自定义错误报告，便于直观查看问题。

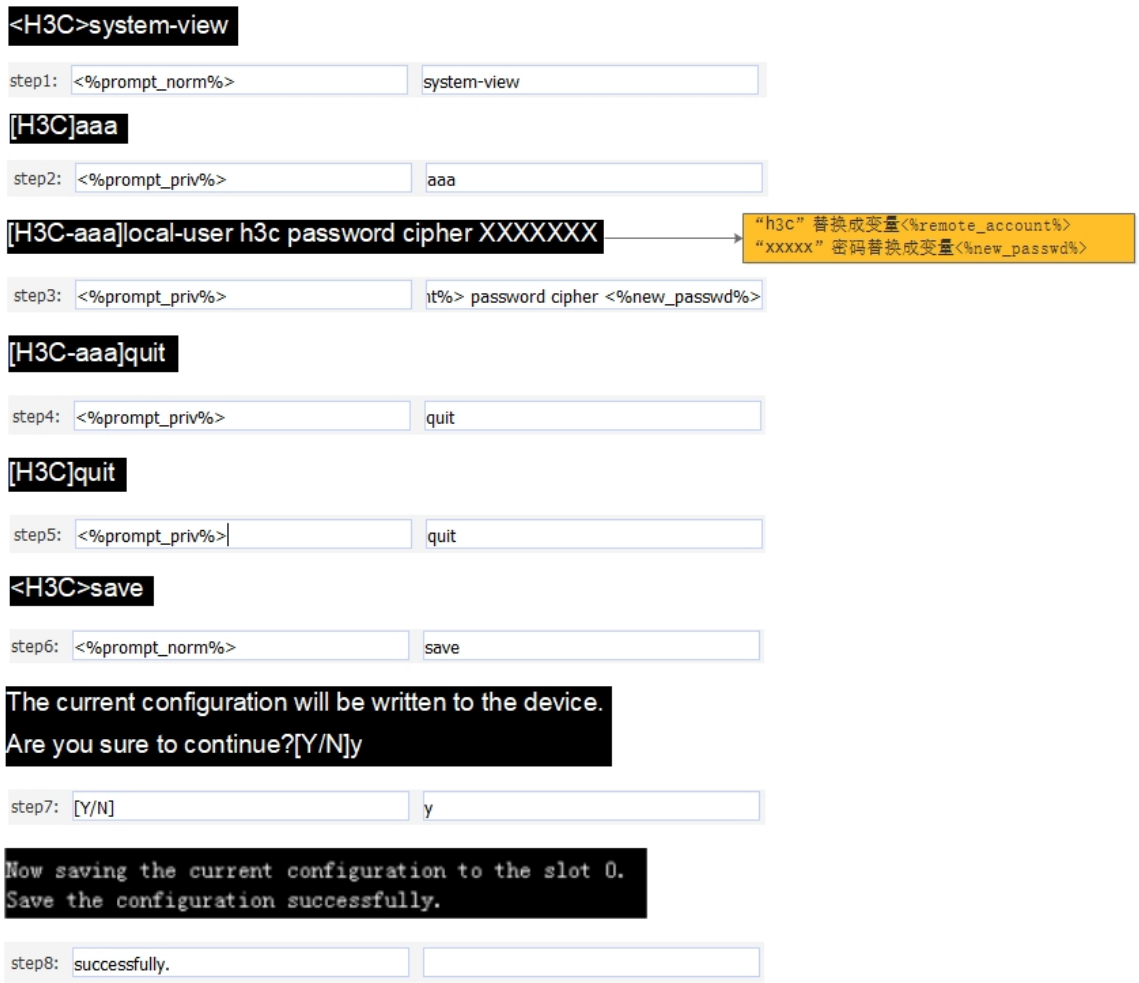
提示

特权账号是指目标设备上的高权限的账户，该账户可以进行高权限的操作，例如账户管理、系统管理等。

例如：linux 设备的 root 账户、windows 的 administrator 账户。

2.2 网络设备改密举例

图2-3 网络设备改密举例



2.3 改密匹配错误内容举例

例如，匹配到了如下内容，将导致改密失败。需要配置“error_expect：”字段。

图2-4 改密出错举例

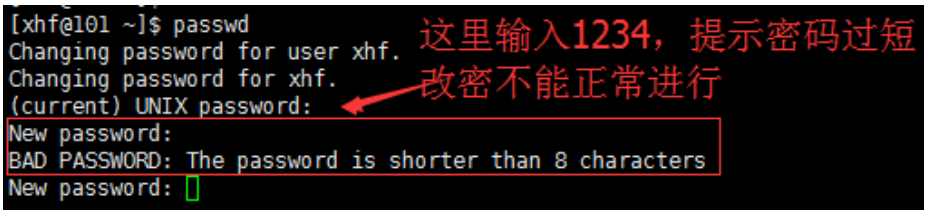
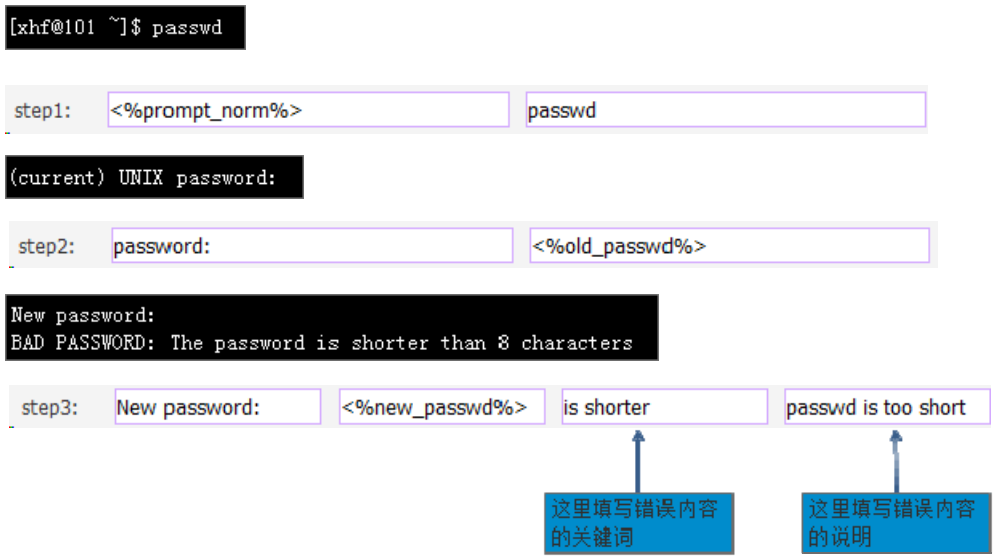


图2-5 配置捕获改密出错



3 自定义改密脚本应用

自定义改密脚本配置好后，需要配置设备类型以及目标设备才能使用。

3.1 配置设备类型

(1) 进入超级管理员账户。

(2) 点击“策略配置”-“设备类型”。

(3) 可以新建设备类型，或者在已存在的设备类型上更换改密方式。

图3-1 设备类型路径

修改改密方式为自定义的改密脚本。

图3-2 修改改密方式

3.2 配置目标设备

(1) 进入配置管理员。

(2) 点击“基本控制”-“目标设备”。

(3) 编辑相应设备。

图3-3 目标设备路径

修改设备类型为之前配置的类型。

图3-4 修改设备类型

4 常见问题

(1) 自定义改密是如何判断改密结束的？

答：所有步骤的 expect 内容匹配，认为改密结束。

(2) 改密过程如何调试？

答：超级管理员-策略设置-字符终端-改密调试信息。

然后重新执行改密计划，会出现调试信息。

(3) 如果一个设备每个账号的改密方式都不一样，如何配置？

答：自定义改密脚本中可以针对不同账号，设置不同的改密方式。

点击“增加账号配置”即可。

(4) 遇见特殊字符，无法匹配，怎么办？

答：这是因为特殊字符需要转义导致的。可以输入“\”，进行转义。

需要转义的字符为：*()+?/.\[=

例如：(current) UNIX password，需转义成：\(current\) UNIX password

(5) 设备登陆等待时间较长，经常超时，怎么办？

答：可以修改“字符终端”-“自动登录超时”来延长改密的等待时间。

(6) 配置网络设备需要注意些什么？

答：一般网络设备在配置完成后，需要保存配置。需要将保存配置这个过程也加入自定义改密脚本。