使用sudo在非root权限下运行jupyterhub

**Overview**

JupyterHub有许多Authenticator和Spawners可用。 某些（如DockerSpawner或OAuthenticator）不需要任何提升的权限。 本文档描述了如何在共享系统上将笔记本服务器作为真实系统用户运行时获取JupyterHub的完全默认行为，而无需以root身份运行Hub本身。

由于JupyterHub需要像其他用户一样生成进程，最简单的方法是以root身份运行它，使用setuid生成用户服务器。 但这并不是特别安全，因为您有一个以root身份在公共Web上运行的进程。

在保留功能的同时运行服务器的一种更谨慎的方法是创建一个专用用户，其sudo访问权限仅限于启动和监视单用户服务器。

**Create a user**

要执行此操作，请首先创建将运行Hub的用户

sudo useradd rhea

此用户不应具有登录shell或密码（可以使用-r）。

**Set up sudospawner**

接下来，您将需要sudospawner来启用使用sudo监控单用户服务器：

sudo python3 -m pip install sudospawner

现在我们必须配置sudo以允许Hub用户（rhea）代表我们的中心用户启动sudospawner脚本（这里是zoe和wash）。 我们希望将这些权限仅限于我们真正需要的权限。

**Edit /etc/sudoers**

为此，我们添加到/ etc / sudoers（使用visudo来安全编辑sudoers）：

* 指定rhea可以为其生成服务器的用户JUPYTER\_USERS列表
* 设置rhea可以代表用户执行的命令JUPYTER\_CMD
* 给rhea权限代表JUPYTER\_USERS运行JUPYTER\_CMD而不输入密码

*# comma-separated whitelist of users that can spawn single-user servers# this should include all of your Hub users*

Runas\_Alias JUPYTER\_USERS = rhea, zoe, wash

*# the command(s) the Hub can run on behalf of the above users without needing a password# the exact path may differ, depending on how sudospawner was installed*

Cmnd\_Alias JUPYTER\_CMD = /usr/local/bin/sudospawner

*# actually give the Hub user permission to run the above command on behalf# of the above users without prompting for a password*

rhea ALL=(JUPYTER\_USERS) NOPASSWD:JUPYTER\_CMD

修改secure\_path以在路径中添加命令可能很有用。

作为将每个用户添加到/ etc / sudoers文件的替代方法，您可以使用上面最后一行中的组，而不是JUPYTER\_USERS：

rhea ALL=(%jupyterhub) NOPASSWD:JUPYTER\_CMD

如果存在jupyterhub组，则无需再次编辑/ etc / sudoers。 添加到组中后，新用户将获得对该应用程序的访问权限：

$ adduser -G jupyterhub newuser

Test sudo setup

测试新用户无需输入密码即可运行sudospawner命令。

这应该提示您的密码切换到rhea，但不提示第二个交换机的任何密码。 它应显示有关日志记录选项的一些帮助输出：

$ sudo -u rhea sudo -n -u $USER /usr/local/bin/sudospawner --help

Usage: /usr/local/bin/sudospawner [OPTIONS]

Options：

--help show this help information

...

这应该失败：

$ sudo -u rhea sudo -n -u $USER echo 'fail'

sudo: a password is required