A+

如何使用rbash限制用户访问Linux系统指定命令

我的一位朋友问我如何允许用户只执行某些任务，并执行某些命令。用户不应更改环境变量/路径，不能访问除主目录以外的其他目录，不能切换到其他用户等。系统管理员分配的少量命令。那可能吗？是! 这是**Restricted Shell**提供帮助的地方。使用Restricted Shell，我们可以轻松限制用户对Linux系统的访问。将用户置于后，只允许他们执行有限的命令集。

在这个简短的教程中，我们将讨论如何在Linux中执行此操作。我在CentOS 7 minimal服务器上测试了这个指南。但是，它适用于大多数类Unix的发行版。

使用受限Shell限制用户对Linux系统的访问

什么是Restricted Shell?

首先，让我澄清一下Restricted Shell究竟是什么。它不是像Bash，Korn Shell等单独的shell。如果使用“rbash”，“- restricted”，“- r”选项启动任何现么它将成为Restricted shell。例如，Bourne shell可以使用命令**bsh -r**作为受限shell启动，使用命令**ksh -r**启动Korn shell 。

Restricted Shell将限制用户执行大多数命令和更改当前工作目录。Restricted Shell将对用户施加以下限制。

- 它不允许您执行**cd**命令。所以你不能去任何地方。您可以简单地留在当前的工作目录中。
- 它不允许您修改 **$ PATH**，**$ SHELL**，**$ BASH_ENV**或**$ ENV**环境变量的值。
- 它不允许您执行包含/（斜杠）字符的程序。例如，您无法运行**/ usr / bin / uname**或**./uname**命令。但是，您可以执行uname命令。换句话说，您只能在中运行命令。
- 您无法使用'重定向输出'>'，'> |'，'<>'，'>＆'，'＆>'，'和'>>'重定向运算符。
- 它不允许您在脚本中退出受限制的shell模式。
- 它不允许您使用**'set + r'**或**'set + o restricted'**关闭受限制的shell模式。

当大量用户使用共享系统时，这非常有用。因此，如果您希望允许用户仅执行特定命令，则**Restricted Shell**是执行此操作的一种方法。

使用Restricted Shell模式

首先，从Bash 创建一个名为**rbash**的符号链接，如下所示。以**root**用户身份运行以下命令。

```
# ln -s /bin/bash /bin/rbash
```

接下来，创建一个名为**“xubo”**的用户，将**rbash**作为他/她的默认登录shell。

```
# useradd xubo -s /bin/rbash
```

设置xubo的密码

```
# passwd xubo
```

在新用户的主文件夹中创建**bin**目录。

```
# mkdir /home/xubo/bin
```

现在，我们需要指定用户可以运行的命令。

在这里，我将让用户只运行**“ls”**，**“mkdir”**和**“ping”**命令。您可以指定您选择的任何命令。

为此，请运行以下命令：

```
# ln -s /bin/ls /home/xubo/bin/ls
```

```
# ln -s /bin/mkdir /home/xubo/bin/mkdir
```

```
# ln -s /bin/ping /home/xubo/bin/ping
```

现在，您了解为什么我们在前面的步骤中创建了“bin”目录。除上述三个命令外，用户无法运行任何命令。

接下来，阻止用户修改**.bash_profile**。

```
# chown root. /home/xubo/.bash_profile
```

```
# chmod 755 /home/xubo/.bash_profile
```

编辑/home/xubo/.bash_profile文件：

```
# vi /home/xubo/.bash_profile
```

修改PATH变量，如下所示。

```
PATH=$HOME/bin
```

Save and close the file by pressing **ESC** key followed by **:wq**.

Now when the user logs in, the restricted shell(rbash) will run as the default login shell and read the **.bash_profile**, which will set PATH to **$HOME** e user will only be able to run the **ls**, **mkdir** and **ping** commands. The restricted shell will not allow the user to change **PATH**, and the permissions on **.** ill not allow the user to alter the environment to bypass the restrictions during the next login session.

Verifying Rbash

Now, log out from root user and log in to the newly created user i.e ostechnix in our case.

Then, run some commands to check whether it works or not. For example, I want to clear the Terminal.

按**ESC**键，然后按：**wq**保存并关闭文件。

现在，当用户登录时，受限shell（rbash）将作为默认登录shell运行并读取**.bash_profile**，它将PATH设置为**$ HOME / bin ,** 以便用户只能运行**ls**，**mkdir**和制的shell将不允许用户更改**PATH**，并且**.bash_profile**上的权限将不允许用户在下次登录会话期间更改环境以绕过限制。

验证Rbash

现在，从root用户注销并登录到新创建的用户，即我们的例子中的xubo。

然后，运行一些命令来检查它是否有效。例如，我想清除终端。

```
$ clear
```

如下:

```
-rbash: clear: command not found
```

您不能使用cd命令更改到不同的目录。

```
$ cd /root
```

如下：

```
-rbash: cd: restricted
```

您也不能使用>运算符重定向输出。

```
$ cat > file.txt
```

如下:

```
-rbash: file.txt: restricted: cannot redirect output
```

允许用户“xubo”仅使用您分配的命令（系统管理员，当然）。在我们的例子中，用户可以执行ls，mkdir和ping命令。

```
$ ls
```

```
$ mkdir dir1
```

```
$ ping www.baiked.com
```

除了这三个命令之外，用户无法做任何事情。他/她完全在你的控制之下。如果要为他/她分配更多命令，请再次登录root用户并分配命令，如下所示。

例如，我想让他/她执行**rm**命令，所以我以root用户身份运行以下命令。

```
# ln -s /bin/rm /home/xubo/bin/rm
```

Rbash手册页

linux rbash