Linux虚拟机的SSH双重登录认证

* 背景介绍

默认情况下，通过SSH登录Linux虚拟机的方式有两种，密码方式和密钥方式。但是对于系统安全环境又较高要求的话，上述两种验证方式还不太够，如果加上一个动态安全口令，那么虚拟机被恶意侵入的概率就要降低很多。以下内容给大家介绍如何利用谷歌身份验证器（开源模块）来实施一次性通行码来验证登录虚拟机。

Important：以下范例基于Azure平台部署的Ubuntu16.04 LTS，如果您使用的是其他版本的Linux操作系统，请注意其中的差异性。

Warning：以下配置涉及到SSH远程连接服务，请在修改前备份好文件，如果配置有误，遇到无法连接问题时，请通过挂盘的方式恢复配置文件，或者致电Azure技术支持中心获取帮助。

* 方案介绍
  + **环境准备**
    - **客户端和服务器端配置为密钥方式免密码登录.**
    - **通过应用商店下载谷歌身份验证器APP.**
* **操作步骤**

1. **以管理员身份登录Ubuntu虚拟机.**
2. **更新Ubuntu软件源：**

**# apt-get update**

1. **安装谷歌身份验证器模块：**

**# apt-get install libpam-google-authenticator**

1. **初始化谷歌身份验证模块：**

**# google-authenticator**

**Do you want authentication tokens to be time-based (y/n) y**

**https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/root@ggauthtest%3Fsecret%3DRI3THQBRYFXPDOJ2**



**Your new secret key is: RI3THQBRYFXPDOJ2**

**Your verification code is 202364**

**Your emergency scratch codes are:**

**58725090**

**14570214**

**59915038**

**35059364**

**13758057**

**Do you want me to update your "/root/.google\_authenticator" file (y/n) y**

**Do you want to disallow multiple uses of the same authentication**

**token? This restricts you to one login about every 30s, but it increases**

**your chances to notice or even prevent man-in-the-middle attacks (y/n) y**

**By default, tokens are good for 30 seconds and in order to compensate for**

**possible time-skew between the client and the server, we allow an extra**

**token before and after the current time. If you experience problems with poor**

**time synchronization, you can increase the window from its default**

**size of 1:30min to about 4min. Do you want to do so (y/n) n**

**If the computer that you are logging into isn't hardened against brute-force**

**login attempts, you can enable rate-limiting for the authentication module.**

**By default, this limits attackers to no more than 3 login attempts every 30s.**

**Do you want to enable rate-limiting (y/n) y**

1. **打开手机端谷歌身份验证器app，扫描上述条形码添加一次性通行码.**
2. **编辑文件/etc/ssh/sshd\_config,**

**将行**

**ChallengeResponseAuthentication no**

**改为**

**ChallengeResponseAuthentication yes**

**在文件末尾添加如下内容：**

**AuthenticationMethods publickey,password publickey,keyboard-interactive**

1. **保存并退出.**
2. **编辑文件/etc/pam.d/sshd,在文件末尾添加如下内容：**

**auth required pam\_google\_authenticator.so**

**同时修改/etc/pam.d/sshd文件中的行：**

**@include common-auth**

1. **保存并退出.**
2. **重启ssh服务：**

**# systemctl restart sshd.service**

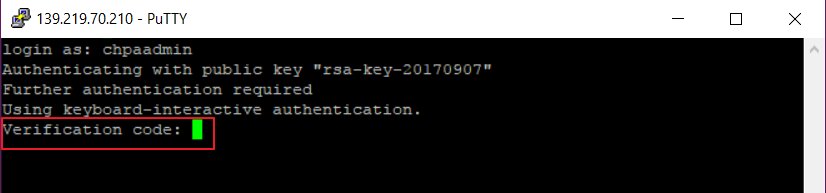
1. **至此，整个谷歌身份验证模块的配置完成。**

* **范例与说明**
  + **每一个登录用户都需要执行命令：**

**# google-authenticator**

**来获取该用户的一次性通行码，将其添加到谷歌身份验证器手机APP上.**

* + **以下是一个范例，供参考：**



**在手机端打开谷歌身份验证器，获取口令：**

