Table Of Contents

Home > Faq > CentOS

CentOS / RedHat: Set Password Quality Requirements

Posted by Vivek Gite <vivek@nixcraft.com>

I've created a unique default group for each user and also used Linux groups to enhance security. Further a group called "users" allowed to login via ssh. However, I need to enforce password quality-control for all users. How do I create a password policy and enforce its use under CentOS or RHEL 5.x server operating systems? [1]

You can use PAM (Pluggable Authentication Modules) to configure a simple password strength checking and password changing policies for all users. /etc/pam.d/system-auth provides important settings for system authentication. [2]

1. **pam_cracklib** - It is a simple password strength checking module for PAM. In addition to checking regular passwords, it offers support for passphrases and can provide randomly generated ones.
2. **pam_passwdqc** - This module provides functionality for only one PAM management group: password changing. In terms of the module-type parameter, this is the "password" feature.
3. **pam_chauthtok()** - Service function may ask the user for a new password, and verify that it meets certain minimum standards. If the chosen password is unsatisfactory, the service function returns PAM_AUTHTOK_ERR.

Setup Strength Checking For Passwords

[3]

The default pam_cracklib PAM module provides strength-checking for passwords. It rejects the password if any one of the following conditions found:

- **Palindrome** - Is the new password a palindrome of the old one?
- **Case Change Only** - Is the new password the the old one with only a change of case?
- **Similar** - Is the new password too much like the old one?
- **Simple** - Is the new password too small?
- **Rotated** - Is the new password a rotated version of the old password?
- Already used - Was the password used in the past? Previously used passwords are to be found in /etc/security/opasswd.

See how to setup check passwords against a dictionary [4] attack using pam_cracklib.

WARNING! These examples may crash your computer if executed. Be careful when making changes to PAM's configuration files. Make sure you first test all options using the sandbox environment.

How To Use pam_passwdqc - Password Quality-control PAM Module

Edit the file /etc/pam.d/system-auth:

```
# cp /etc/pam.d/system-auth /root/backup/system-auth
# vi /etc/pam.d/system-auth
```

Find the line:

```
password    requisite     pam_cracklib.so try_first_pass retry=3
```

and replace it with the following line:

```
password    requisite    pam_passwdqc.so min=disabled,disabled,12,8,7 retry=3
```

Where,

- **min=N0,N1,N2,N3,N4 - min=disabled,disabled,12,8,7 is the password policy. Each filed (N0,N1..N4) is used for different purpose. The keyword disabled can be used to disallow passwords of a given kind regardless of their length. Each subsequent number is required to be no larger than the preceding one. N0 is used for passwords consisting of characters from one character class only. The character classes are - digits, lower-case letters, upper-case letters, and other characters.**
    1. **N1 is used for passwords consisting of characters from two character classes which do not meet the requirements for a passphrase.**
    2. **N2 is used for passphrases. A passphrase must consist of sufficient words (see the passphrase option below).**
    3. **N3 and N4 are used for passwords consisting of characters from three and four character classes, respectively.**
    4. **When calculating the number of character classes, upper-case letters used as the first character and digits used as the last character of a password are not counted.**
    5. **In addition to being sufficiently long, passwords are required to contain enough different characters for the character classes and the minimum length they have been checked against.**
    6. **retry=3 - The number of times the module will ask for a new password if the user fails to provide a sufficiently strong password and enter it twice the first time.**

See the help file /usr/share/doc/pam_passwdqc-1.0.2/README and the man page pam_passwdqc for detailed configuration options.

How Do I Lockout User Accounts?

You need to use the pam tally2 PAM module which [5] provides the capability to lock out user accounts after a number of failed login attempts.

References:

- The Linux-PAM Guides [6]

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/rhel-fedora-centos-linux-password-quality-control/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/centos/**
[2] Image: **http://www.cyberciti.biz/faq/category/redhat-and-friends/**
[3] Image: **http://www.cyberciti.biz/faq/category/fedora-linux/**
[4] check passwords against a dictionary: **http://www.cyberciti.biz/tips/linux-check-passwords-against-a-dictionary-attack.html**
[5] pam tally2 PAM module which: **http://www.cyberciti.biz/tips/lock-unlock-set-number-of-login-attempts.html**
[6] The Linux-PAM Guides: **http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/**