Table Of Contents

Home > Faq > CentOS

Linux Upgrade Password Hashing Algorithm to SHA-512

Posted by Vivek Gite <vivek@nixcraft.com>

The default algorithm for storing password hashes in /etc/shadow [2] is MD5. I was told to use SHA-512 hashing algorithm. How do I set password hashing using the SHA-256 and SHA-512 under CentOS or Redhat Enterprise Linux 5.4?

You need to use authconfig command to setup SHA-256/512 hashing. This command provides a simple method of configuring /etc/sysconfig/network to handle NIS, as well as /etc/passwd and /etc/shadow, the files used for shadow password support. Basic LDAP, Kerberos 5, and SMB (authentication) client configuration is also provided.

[1]

Display Current Hashing Algorithm

Type the following command:

```
# authconfig --test | grep hashing
```

Sample outputs:

```
password hashing algorithm is md5
```

Configure Linux Server To Use The SHA-512

To configure the Linux system to use the SHA-512 algorithm, enter:

```
# authconfig --passalgo=sha512 --update
```

Note users need to change their passwords in order to generate hashes using SHA-512. You can force users to change their password [3] on next login:

```
# chage -d 0 userName
```

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our daily email newsletter or weekly newsletter to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

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

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

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/linux/**
[2] /etc/shadow: **http://www.cyberciti.biz/faq/understanding-etcshadow-file/**
[3] change their password: **http://www.cyberciti.biz/faq/rhel-debian-force-users-to-change-passwords/**