Set a password policy in Red Hat Enterprise Linux 7

https://access.redhat.com/solutions/2808101

Medio Ambiente

* Red Hat Enterprise Linux 7 * pam_pwquality.so * pam_pwhistory.so

Cuestión

Requirement 1. Keep history of used passwords (the number of previous passwords which cannot be reused)

Requirement 2. Password size (Minimum acceptable size for the new password).

Requirement 3. Set limit to number of digits in password.

Requirement 4. Set limit to number of Upper Case characters in password.

Requirement 5. Set limit to number of Lower Case characters in password.

Requirement 6. Set limit to number of Other characters in password.

Requirement 7. Set minimum number of required classes in new password (digits, uppercase, lowercase, others).

Requirement 8. Set maximum number of allowed consecutive same characters in the new password.

Requirement 9. A maximum number of allowed consecutive characters of the same class in the new password.

Requirement 10. A maximum number of characters that is allowed to use in new passwords(compared to old password).

Requirement 11. Enforce root for password complexity.

Resolución

- In Red Hat Enterprise Linux 7 default configuration file for password complexity `/etc/security/pwquality.conf` .
- **Requirement 1**: Keep history of passwords used
    - Insert the following in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` (after `pam_pwquality.so` line):

      ```
      password    requisite     pam_pwhistory.so remember=5 use_authtok
      ```

- **Requirement 2**: minlen = 9(minimum length of a password)
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      minlen = 9
      ```

- **Requirement 3**: dcredit=1(number of digits in password).
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      dcredit = 1
      ```
- **Requirement 4**: ucredit = 1(number of Upper Case character in password)
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      ucredit = 1
      ```
- **Requirement 5**: lcredit = 1(number of Lower Case character in password)
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      lcredit = 1
      ```
- **Requirement 6**: ocredit = 1(number of Lower Case character in password)
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      ocredit = 1
      ```
- **Requirement 7**: minclass = 1(number of required classes character in new password)
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      minclass = 1
      ```
- **Requirement 8**: maxrepeat = 2 (maximum number of allowed consecutive same characters in the new password)
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      maxrepeat = 2
      ```
- **Requirement 9**: maxclassrepeat = 2 (maximum number of allowed consecutive characters of the same class in the new password)
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      maxclassrepeat = 2
      ```
- **Requirement 10**: A maximum number of characters that is allowed to use in new passwords(compared to old password).
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      difok = 5
      ```
- **Requirement 11**: Requirement 11. Enforce root for password complexity.
    - Insert the following option in `/etc/security/pwquality.conf`:

      ```
      enforce_for_root
      ```
- For more information refer man page of **pwquality.conf**.

  ```
  # man pwquality.conf
  ```