목차

root 계정 원격 접속 제한 3
Root ssh login 제한 5
패스워드 복잡성 설정 5
계정 잠금 임계값 설정 9
패스워드 파일 보호 12
root 계정 su 제한 12
패스워드 최소 길이, 최대 사용 기간, 최소 사용기간 설정 13
불필요한 계정 제거 13
관리자 그룹에 최소한의 계정 포함 13
계정이 존재하지 않는 GID 금지 13
동일한 UID 금지 13
사용자 shell 점검 13
Session Timeout 설정 13

root 계정 원격 접속 제한

항목 중요도 상

점검목적 관리자계정 탈취로 인한 시스템 장악을 방지하기 위해 외부 비인가자의 root 계정 접근 시도를 원천적으로 차단하기 위함

보안위협 root 계정은 운영체제의 모든기능을 설정 및 변경이 가능하여(프로세스, 커널변경 등) root 계정을 탈취하여 외부에서 원격을 이용한 시스템 장악 및 각종 공격으로(무작위 대입 공격) 인한 root 계정 사용 불가 위협

점검방법

RHEL 6, 7

[Telnet]

```
#cat /etc/pam.d/login
auth required /lib/security/pam_securetty.so
#cat /etc/securetty
pts/0 ~ pts/x 관련 설정이 존재하지 않음
```

[Telnet 서비스 사용시] Step 1) `/etc/securetty` 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리
Step 2) `/etc/pam.d/login` 파일 수정 또는, 신규 삽입

```
(수정 전) #auth required /lib/security/pam_securetty.so
(수정 후) auth required /lib/security/pam_securetty.so
```

※ /etc/securetty : Telnet 접속 시 root 접근 제한 설정 파일 `/etc/securetty` 파일 내 *pts/x 관련 설정이 존재하는 경우 PAM 모듈 설정과 관계없이 root 계정 접속을 허용하므로 반드시 `/etc/securetty` 파일에서 pts/x 관련 설정 제거 필요

또는

```
#echo > /etc/securetty
```

위에 제시한 내용으로 설정되어 있을 경우 root 원격 접속이 차단됨 / 내용 설정에 대해서는 아래의 보안 설정방법을 참고함

결과

```
Last login: Fri Jan  7 14:27:23 2022 from 192.168.230.1
[root@rhel7 ~]# telnet 192.168.230.143
Trying 192.168.230.143...
Connected to 192.168.230.143.
```

```
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.10 (Santiago)
Kernel 2.6.32-754.el6.x86_64 on an x86_64
rhel6 login: root
Password:
Login incorrect
```

[SSH 서비스 사용시]

Step 1) vi 편집기를 이용하여 `/etc/ssh/sshd_config` 파일 열기 Step 2) 아래와 같이 주석 제거 또는, 신규 삽입

```
(수정 전) #PermitRootLogin Yes
(수정 후) PermitRootLogin No
```

루트 계정에 대한 액세스를 추가로 제한하기 위해 관리자는 `/etc/securetty` 파일을 편집하여 콘솔에서 루트 로그인을 비활성화할 수 있습니다. 기본적으로 Red Hat Enterprise Linux의 `/etc/securetty` 파일은 루트 사용자가 시스템에 물리적으로 연결된 콘솔에서만 로그인할 수 있도록 허용합니다. 루트 사용자가 로그인하지 못하도록 하려면 쉘 프롬프트에서 루트로 다음 명령을 입력하여 이 파일의 내용을 제거하십시오.

```
echo > /etc/securetty
```

KDM, GDM 및 XDM 로그인 관리자에서 securetty 지원을 활성화하려면 다음 행을 추가하십시오.

```
auth [user_unknown=ignore success=ok ignore=ignore default=bad]
pam_securetty.so
```

위 설정을 적용하기 위한 파일들은 다음과 같습니다.

```
/etc/pam.d/gdm
/etc/pam.d/gdm-autologin
/etc/pam.d/gdm-fingerprint
/etc/pam.d/gdm-password
/etc/pam.d/gdm-smartcard
/etc/pam.d/kdm
/etc/pam.d/kdm-np
/etc/pam.d/xdm
```

참조링크
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index#s2-wstation-privileges-noroot

RHEL 8 이후 시스템에서 tty 장치 파일의 동적 특성으로 인해 securetty PAM 모듈은 기본적으로 비활성화되었으며 /etc/securetty 구성 파일은 더 이상 RHEL에 포함되지 않습니다. /etc/securetty는 가능한 많

은 장치를 나열하므로 대부분의 경우 실질적인 효과는 기본적으로 허용되는 것이므로 이 변경은 약간의 영향만 미칩니다. 그러나 보다 제한적인 구성을 사용하는 경우 /etc/pam.d 디렉토리의 해당 파일에 pam_securetty.so 모듈을 활성화하는 행을 추가하고 새 /etc/securetty 파일을 생성해야 합니다.

참조링크
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/considerations_in_adopting_rhel_8/security_considerations-in-adopting-rhel-8#securetty_security

Root ssh login 제한

RHEL 6, 7

SSH 프로토콜을 사용한 루트 로그인을 방지하려면 SSH 데몬의 구성 파일 `/etc/ssh/sshd_config`를 편집하고 다음 행을 변경하십시오.

```
#PermitRootLogin yes
PermitRootLogin no
```

참조링크
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index#s2-wstation-privileges-noroot

RHEL 8

```
#PermitRootLogin yes
PermitRootLogin no
```

PermitRootLogin 옵션 no - root 계정의 모든 접근 방법을 차단 prohibit-password - root 계정의 암호를 사용하는 대신 키 기반 인증은 가능함

참조링크
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/securing_networks/index

패스워드 복잡성 설정

RHEL 6

네 가지 문자 클래스를 모두 포함하여 최소 길이가 8자인 암호를 요구하려면 /etc/pam.d/passwd 파일의 암호 섹션에 다음 줄을 추가하십시오.

```
password   required     pam_cracklib.so retry=3 minlen=8 minclass=4
```

연속 또는 반복 문자에 대한 암호 강도 검사를 설정하려면 /etc/pam.d/passwd 파일의 암호 섹션에 다음 줄을 추가합니다.

```
password   required     pam_cracklib.so retry=3 maxsequence=3 maxrepeat=3
```

참조링크
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index#sect-Security_Guide-Workstation_Security-Password_Security

RHEL 7

pam_quality 사용을 활성화하려면 /etc/pam.d/passwd 파일의 암호 스택에 다음 줄을 추가합니다.

```
password    required    pam_pwquality.so retry=3
```

네 가지 문자 클래스를 모두 포함하여 최소 길이가 8자인 암호를 요구하려면 /etc/security/pwquality.conf 파일에 다음 행을 추가하십시오.

```
minlen = 8
minclass = 4
```

문자 시퀀스 및 동일한 연속 문자에 대한 암호 강도 검사를 설정하려면 /etc/security/pwquality.conf에 다음 행을 추가하십시오.

```
maxsequence = 3
maxrepeat = 3
```

참조문서
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/security_guide/index

RHEL 8

Red Hat Enterprise Linux 8에서는 authconfig명령이 authselect 유틸리티로 대체되었습니다. `/etc/pam.d/` 디렉토리에 있는 PAM 전역 파일 system-auth 및 password-auth에서 직접 수정하지 않는 것이 좋습니다.

Red Hat Enterprise Linux 8에서 암호 복잡성에 대한 기본 구성 파일은 `/etc/security/pwquality.conf` 비밀번호 정책/복잡성을 구성하기 전에 아래와 같이 authselect를 사용하여 사용자 정의 프로파일을 작성하십시오.

1. 사용 가능한 프로필 나열

```
# authselect list
```

2. 현재 프로필 및 활성화된 기능 나열

```
# authselect current
```

3. 현재 프로필/변경 사항 백업

```
# authselect apply-changes -b --backup=sssd.backup
```

4. 기존 프로필 sssd에서 복사한 새 사용자 지정 프로필 이름 password-policy 생성

```
#  authselect create-profile password-policy -b sssd
```

- 새로 생성된 프로필은 /etc/authselect/custom/password-policy/ 위치에서 사용할 수 있습니다.

5. 새 사용자 정의 프로필을 현재 프로필로 설정

```
# authselect select custom/password-policy
# authselect current
```

6. 예를 들어 기능을 활성화하려면 사용자 로그인 시 홈 디렉토리가 아직 없는 경우 생성하고 faillock을 사용하여 계정 잠금을 활성화하려면 다음 명령을 실행합니다.

```
# authselect enable-feature with-mkhomedir
# authselect enable-feature with-faillock
```

RHEL 8.2 릴리스에서 `pam_faillock`은 이제 `/etc/security/faillock.conf`에 있는 `faillock.conf` 구성 파일에서 설정을 읽을 수 있습니다. 이 페이지의 아래 참고 사항을 참조하십시오.

메모: `/etc/pam.d/xxxx-auth`의 `pam_faillock.so` 행에 있는 옵션은 `faillock.conf`의 설정을 재정의합니다. `faillock.conf`에서 구성하려면 다음과 같이 `/etc/authselect/custom/PROFILE/xxxx-auth`를 수정하십시오.

```
# Edit {system,password,fingerprint,smartcard}-auth in
/etc/authselect/custom/password-policy/

(Before)
auth        required                                        pam_env.so
auth        required                                        pam_faildelay.so
delay=2000000
auth        required                                        pam_faillock.so
```

```
preauth silent deny=4 unlock_time=1200
...snip...
auth        required                                        pam_faillock.so
authfail deny=4 unlock_time=1200
auth        required                                        pam_deny.so
↓
(After)
auth        required                                        pam_env.so
auth        required                                        pam_faildelay.so
delay=2000000
auth        required                                        pam_faillock.so
preauth
...snip...
auth        required                                        pam_faillock.so
authfail
auth        required                                        pam_deny.so
```

7. 사용자 정의 프로필 디렉토리 `/etc/authselect/custom/password-policy/`에서 사용할 수 있는 전역 PAM 구성 파일 `system-auth` 및 `password-auth`에서 원하는/사용자 정의 변경을 수행합니다. 변경 사항이 적용되면 다음 명령을 사용하여 적용합니다.

```
# authselect apply-changes
```

- 파일에 변경 사항이 기록되었는지 확인합니다.

8. 사용된 비밀번호의 이력(재사용할 수 없는 이전 비밀번호의 수)을 유지합니다. `/etc/authselect/custom/password-policy/system-auth` 및 `/etc/authselect/custom/password-policy/password-auth` 파일에 다음 줄을 삽입합니다(pam_pwquality.so 줄 뒤에)

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

9. 암호 복잡성을 위해 루트를 적용합니다. `/etc/authselect/custom/password-policy/system-auth` 및 `/etc/authselect/custom/password-policy/password-auth` 파일의 암호 섹션 아래 `pam_pwquality.so` 행에 다음 옵션을 삽입/추가합니다.

```
enforce_for_root
```

참고: 변경한 후 변경 사항을 적용하려면 authselect apply-changes를 실행해야 합니다.

10. `/etc/security/pwquality.conf` 파일에서 적절한 옵션을 설정하십시오.

```
minlen = 9          새 암호에 대해 허용되는 최소 크기입니다. 여기에는 크레딧(기본값인 비활
성화되지 않은 경우 1개 추가)이 포함됩니다.
dcredit = -1        비밀번호에 필요한 숫자가 있어야 하는 최소 크레딧
ucredit = -1        비밀번호에 대문자를 사용하기 위한 최소 크레딧입니다.
```

```
lcredit = 1          비밀번호에 소문자를 사용할 수 있는 최대 크레딧입니다.
ocredit = 1          암호에 다른 문자를 포함할 수 있는 최대 크레딧입니다.
minclass = 1         새 비밀번호에 필요한 최소 문자 클래스 수.
maxrepeat = 2        새 비밀번호에서 연속으로 허용되는 동일한 문자의 최대 수입니다.
maxclassrepeat = 2   새 비밀번호에서 동일한 클래스의 연속 문자가 허용되는 최대 수입니다.
difok = 5            새 비밀번호에 사용할 수 있는 최대 문자 수(이전 비밀번호에 비해..),
root는 이전 비밀번호를 묻지 않으므로 적용되지 않음
```

크레딧 값 > 0 : 새 비밀번호에 각 문자를 포함하기 위한 최대 크레딧입니다. 크레딧 값 < 0 : 새 비밀번호에 각 문자를 포함하는 데 필요한 최소 필수 크레딧입니다. 신용 값 = 0: 새 암호에 해당 문자 클래스를 포함해야 하는 필수 요구 사항이 없습니다.

참조링크 https://access.redhat.com/solutions/5027331

계정 잠금 임계값 설정

RHEL 6

3번의 실패한 시도 후에 루트가 아닌 사용자를 잠그고 10분 후에 해당 사용자의 잠금을 해제하려면 /etc/pam.d/system-auth 및 /etc/pam.d/password-의 auth 섹션에 다음 행을 추가하십시오.

```
auth        required       pam_faillock.so preauth silent audit deny=3
unlock_time=600
auth        sufficient     pam_unix.so nullok try_first_pass
auth        [default=die]  pam_faillock.so authfail audit deny=3
unlock_time=600
```

이전 단계에서 지정한 두 파일의 계정 섹션에 다음 줄을 추가합니다.

```
account     required      pam_faillock.so
```

루트 사용자에게도 계정 잠금을 적용하려면 /etc/pam.d/system-auth 및 /etc/pam.d/password-auth 파일의 pam_faillock 항목에 even_deny_root 옵션을 추가합니다.

```
auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root unlock_time=600
auth        sufficient    pam_unix.so nullok try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root unlock_time=600

account     required      pam_faillock.so
```

사용자 계정의 잠금을 해제하려면 루트로 다음 명령을 실행합니다.

```
# faillock --user <username> --reset
```

참조문서
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index#sect-Security_Guide-Workstation_Security-Account_Locking

RHEL 7

3번의 실패한 시도 후에 루트가 아닌 사용자를 잠그고 10분 후에 해당 사용자의 잠금을 해제하려면 /etc/pam.d/system-auth 및 /etc/pam.d/password-auth의 auth 섹션에 두 줄을 추가합니다. 파일. 편집 후 두 파일의 전체 인증 섹션은 다음과 같아야 합니다.

```
1 auth        required      pam_env.so
2 auth        required      pam_faillock.so preauth silent audit deny=3
unlock_time=600  <- 추가
3 auth        sufficient    pam_unix.so nullok try_first_pass
4 auth        [default=die] pam_faillock.so authfail audit deny=3
unlock_time=600  <- 추가
5 auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
6 auth        required      pam_deny.so
```

이전 단계에서 지정한 두 파일의 계정 섹션에 다음 줄을 추가합니다.

```
account     required      pam_faillock.so
```

루트 사용자에게도 계정 잠금을 적용하려면 /etc/pam.d/system-auth 및 /etc/pam.d/password-auth 파일의 auth required pam_faillock.so 항목에 even_deny_root 옵션을 추가합니다.

```
auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root unlock_time=600
auth        sufficient    pam_unix.so nullok try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root unlock_time=600

account     required      pam_faillock.so
```

사용자 계정의 잠금을 해제하려면 루트로 다음 명령을 실행합니다.

```
#faillock --user <username> --reset
```

참조문서
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/security_guide/index#sect-Security_Guide-Workstation_Security-Account_Locking

https://access.redhat.com/solutions/62949

RHEL 8

`/etc/pam.d/system-auth` 및 `/etc/pam.d/password-auth`를 수동으로 편집하는 것은 권장되지 않습니다. `authselect`를 사용하여 `pam_faillock`을 활성화/비활성화합니다.

To enable faillock

```
# authselect enable-feature with-faillock
```

To disable faillock

```
# authselect disable-feature with-faillock
```

faillock 구성 faillock 옵션은 /etc/security/faillock.conf에 저장해야 합니다.

```
deny=4
unlock_time=1200
silent
```

인증 실패 기록을 재설정하거나 보려면 다음과 같은 명령을 사용하십시오. 사용자 이름에 대한 인증 실패 기록을 표시하려면

```
# faillock --user username
```

사용자 이름에 대한 인증 실패 기록을 재설정하려면

```
# faillock --user username --reset
```

SSHD 구성 조정 `pam_faillock.so`가 예상대로 작동하지 않으면 SSHD 구성을 다음과 같이 변경해야 할 수 있습니다.

```
# vi /etc/ssh/sshd_config
ChallengeResponseAuthentication yes
PasswordAuthentication no
```

그런 다음 이러한 구성 변경 사항을 적용하려면 sshd 서비스를 다시 시작합니다.

```
# systemctl restart sshd
```

참조문서 https://access.redhat.com/solutions/62949

패스워드 파일 보호

/etc/shadow 파일의 패스워드 암호화 존재 확인 /etc/passwd 파일 내 두 번째 필드가 " X " 표시되는지 확인

참조문서
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index

root 이외에 UID가 '0' 금지

/etc/passwd 파일 내 UID (세 번째 필드 값) 확인 root 이외의 계정이 "UID=0"인 경우 0이 아닌 적절한 UID 부여

참조문서
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index

root 계정 su 제한

"wheel" 그룹 및 그룹 내 구성원 존재 여부 확인 /etc/group wheel:x:10:root,admin

/etc/pam.d/su

```
#%PAM-1.0
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel"
group.
#auth           sufficient      pam_wheel.so trust use_uid          # 주석해
제 시 해당 그룹사용자는 무조건 신뢰(패스워드확인 안함)
# Uncomment the following line to require a user to be in the "wheel" group.
#auth           required        pam_wheel.so use_uid                # 주석해
제 시 해당 그룹사용자는 패스워드 확인 후 신뢰
auth            include         system-auth
account         sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account         include         system-auth
password        include         system-auth
session         include         system-auth
session         optional        pam_xauth.so
```

참조문서 https://access.redhat.com/solutions/452213

패스워드 최소 길이, 최대 사용 기간, 최소 사용기간 설정

/etc/login.defs 내 패스워드 관련 파일 수정

```
PASS_MAX_DAYS   99999  패스워드 사용 가능 기간(일)
PASS_MIN_DAYS   0      패스워드 변경 최소 기간(일)
PASS_MIN_LEN    5      패스워드 최소 길이
PASS_WARN_AGE   7      패스워드 기간 만료 경고 기간(일)
```

불필요한 계정 제거

/etc/passwd 파일 내 계정확인 후 제거

관리자 그룹에 최소한의 계정 포함

/etc/group 내 root:x:0:root 확인

계정이 존재하지 않는 GID 금지

/etc/group 파일과 /etc/passwd 파일 비교하여 점검

동일한 UID 금지

/etc/passwd 파일 내 동일한 UID가 있는지 확인

사용자 shell 점검

로그인이 불필요한 계정에 /bin/false 또는 /sbin/nologin 쉘 부여

/etc/passwd 파일 내 로그인 쉘 부분인 계정 맨 마지막에 부여

Session Timeout 설정

/etc/profile 파일 내

```
HOSTNAME=`/usr/bin/hostname 2>/dev/null`
HISTSIZE=5000                                   # 히스토리 저장 갯수
HISTTIMEFORMAT="%F %T "                         # 히스토리 저장시 날짜 시간 같이 저장
TMOUT=300                                       # 세션 타임아웃 시간 설정
if [ "$HISTCONTROL" = "ignorespace" ] ; then
    export HISTCONTROL=ignoreboth
```

```
else
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL HISTTIMEFORMAT
TMOUT  # 환경변수 적용
```

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/%EA%B3%84%EC%A0%95%EA%B4%80%EB%A6%AC

Last update: **2022/01/11 07:01**