* 1. **-Linux-操作系统**

### 系统信息

#### 查看系统信息

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-02-01-01** |
| **查看内核信息** | uname -a |
| **检查结果** | Linux localhost.localdomain 3.10.0-1160.42.2.el7.x86\_64 #1 SMP Tue Sep 7 14:49:57 UTC 2021 x86\_64 x86\_64 x86\_64 GNU/Linux |
| **查看所有软件包** | rpm -qa |
| **检查结果** | openssh-server-7.4p1-21.el7.x86\_64 setup-2.8.71-11.el7.noarch authconfig-6.2.8-30.el7.x86\_64 ncurses-base-5.9-14.20130511.el7\_4.noarch biosdevname-0.7.3-2.el7.x86\_64 libstdc++-4.8.5-44.el7.x86\_64 pcre-8.32-17.el7.x86\_64 btrfs-progs-4.9.1-1.el7.x86\_64 xz-libs-5.2.2-1.el7.x86\_64 libsysfs-2.1.0-16.el7.x86\_64 bzip2-libs-1.0.6-13.el7.x86\_64 rootfiles-8.1-11.el7.noarch readline-6.2-11.el7.x86\_64 libattr-2.4.46-13.el7.x86\_64 audit-libs-2.8.5-4.el7.x86\_64 libxml2-2.9.1-6.el7.5.x86\_64 grub2-common-2.02-0.87.el7.centos.6.noarch findutils-4.5.11-6.el7.x86\_64 nss-softokn-freebl-3.53.1-6.el7\_9.x86\_64 sqlite-3.7.17-8.el7\_7.1.x86\_64 nss-util-3.53.1-1.el7\_9.x86\_64 libaio-0.3.109-13.el7.x86\_64 coreutils-8.22-24.el7\_9.2.x86\_64 libassuan-2.1.0-3.el7.x86\_64 glib2-2.56.1-9.el7\_9.x86\_64 libgomp-4.8.5-44.el7.x86\_64 nss-sysinit-3.53.1-7.el7\_9.x86\_64 jansson-2.10-1.el7.x86\_64 openldap-2.4.44-24.el7\_9.x86\_64 tcp\_wrappers-libs-7.6-77.el7.x86\_64 dhcp-common-4.2.5-83.el7.centos.1.x86\_64 ethtool-4.8-10.el7.x86\_64 python-firewall-0.6.3-13.el7\_9.noarch newt-0.52.15-4.el7.x86\_64 freetype-2.8-14.el7\_9.1.x86\_64 less-458-9.el7.x86\_64 libsmartcols-2.23.2-65.el7\_9.1.x86\_64 ipset-7.1-1.el7.x86\_64 grub2-tools-minimal-2.02-0.87.el7.centos.6.x86\_64 bc-1.06.95-13.el7.x86\_64 grub2-tools-extra-2.02-0.87.el7.centos.6.x86\_64 kmod-libs-20-28.el7.x86\_64 virt-what-1.18-4.el7\_9.1.x86\_64 libselinux-utils-2.5-15.el7.x86\_64 kernel-3.10.0-1160.42.2.el7.x86\_64 gmp-6.0.0-15.el7.x86\_64 lvm2-2.02.187-6.el7\_9.5.x86\_64 libverto-0.2.5-4.el7.x86\_64 sudo-1.8.23-10.el7\_9.1.x86\_64 p11-kit-trust-0.23.5-3.el7.x86\_64 NetworkManager-wifi-1.18.8-2.el7\_9.x86\_64 curl-7.29.0-59.el7\_9.1.x86\_64 shadow-utils-4.6-5.el7.x86\_64 iwl2000-firmware-18.168.6.1-80.el7\_9.noarch iwl3945-firmware-15.32.2.9-80.el7\_9.noarch cracklib-dicts-2.9.0-11.el7.x86\_64 iwl6000g2a-firmware-18.168.6.1-80.el7\_9.noarch gettext-libs-0.19.8.1-3.el7.x86\_64 iwl5000-firmware-8.83.5.1\_1-80.el7\_9.noarch gobject-introspection-1.56.1-1.el7.x86\_64 ca-certificates-2021.2.50-72.el7\_9.noarch pyliblzma-0.5.3-11.el7.x86\_64 python-configobj-4.7.2-7.el7.noarch pyxattr-0.5.1-5.el7.x86\_64 nss-pem-1.0.3-7.el7.x86\_64 binutils-2.27-44.base.el7.x86\_64 hardlink-1.0-19.el7.x86\_64 libseccomp-2.3.1-4.el7.x86\_64 procps-ng-3.3.10-28.el7.x86\_64 elfutils-libs-0.176-5.el7.x86\_64 dbus-1.10.24-15.el7.x86\_64 iputils-20160308-10.el7.x86\_64 ebtables-2.0.10-16.el7.x86\_64 hwdata-0.252-9.7.el7.x86\_64 dbus-glib-0.100-7.el7.x86\_64 plymouth-core-libs-0.8.9-0.34.20140113.el7.centos.x86\_64 rpm-python-4.11.3-45.el7.x86\_64 yum-3.4.3-168.el7.centos.noarch kbd-1.15.5-15.el7.x86\_64 libgcc-4.8.5-44.el7.x86\_64 openssh-clients-7.4p1-21.el7.x86\_64 filesystem-3.2-25.el7.x86\_64 audit-2.8.5-4.el7.x86\_64 kbd-legacy-1.15.5-15.el7.noarch kernel-3.10.0-1160.el7.x86\_64 chrony-3.4-1.el7.x86\_64 irqbalance-1.0.7-12.el7.x86\_64 ncurses-libs-5.9-14.20130511.el7\_4.x86\_64 parted-3.1-32.el7.x86\_64 libsepol-2.5-10.el7.x86\_64 man-db-2.6.3-11.el7.x86\_64 libselinux-2.5-15.el7.x86\_64 info-5.1-5.el7.x86\_64 xfsprogs-4.5.0-22.el7.x86\_64 libcom\_err-1.42.9-19.el7.x86\_64 sed-4.2.2-7.el7.x86\_64 popt-1.13-16.el7.x86\_64 libdb-5.3.21-25.el7.x86\_64 grep-2.20-3.el7.x86\_64 elfutils-libelf-0.176-5.el7.x86\_64 ivtv-firmware-20080701-26.el7.noarch libacl-2.2.51-15.el7.x86\_64 libcap-ng-0.7.5-4.el7.x86\_64 libgpg-error-1.12-3.el7.x86\_64 libgcrypt-1.5.3-14.el7.x86\_64 cpio-2.11-28.el7.x86\_64 gpg-pubkey-f4a80eb5-53a7ff4b lua-5.1.4-15.el7.x86\_64 centos-release-7-9.2009.1.el7.centos.x86\_64 which-2.20-7.el7.x86\_64 tzdata-2021a-1.el7.noarch libnl3-3.2.28-4.el7.x86\_64 glibc-common-2.17-324.el7\_9.x86\_64 file-libs-5.11-37.el7.x86\_64 nspr-4.25.0-2.el7\_9.x86\_64 libmnl-1.0.3-7.el7.x86\_64 zlib-1.2.7-19.el7\_9.x86\_64 openssl-libs-1.0.2k-21.el7\_9.x86\_64 p11-kit-0.23.5-3.el7.x86\_64 libuuid-2.23.2-65.el7\_9.1.x86\_64 groff-base-1.22.2-8.el7.x86\_64 libmount-2.23.2-65.el7\_9.1.x86\_64 xz-5.2.2-1.el7.x86\_64 python-libs-2.7.5-90.el7.x86\_64 libunistring-0.9.3-9.el7.x86\_64 nss-softokn-3.53.1-6.el7\_9.x86\_64 libedit-3.0-12.20121213cvs.el7.x86\_64 nss-3.53.1-7.el7\_9.x86\_64 libnfnetlink-1.0.1-4.el7.x86\_64 nss-tools-3.53.1-7.el7\_9.x86\_64 hostname-3.13-3.el7\_7.1.x86\_64 libcurl-7.29.0-59.el7\_9.1.x86\_64 lzo-2.06-8.el7.x86\_64 dhcp-libs-4.2.5-83.el7.centos.1.x86\_64 lz4-1.8.3-1.el7.x86\_64 systemd-sysv-219-78.el7\_9.3.x86\_64 keyutils-libs-1.5.8-3.el7.x86\_64 NetworkManager-1.18.8-2.el7\_9.x86\_64 slang-2.2.4-11.el7.x86\_64 python-perf-3.10.0-1160.42.2.el7.x86\_64 libnetfilter\_conntrack-1.0.6-1.el7\_3.x86\_64 bind-export-libs-9.11.4-26.P2.el7\_9.7.x86\_64 iproute-4.11.0-30.el7.x86\_64 dmidecode-3.2-5.el7\_9.1.x86\_64 libteam-1.29-3.el7.x86\_64 vim-minimal-7.4.629-8.el7\_9.x86\_64 ipset-libs-7.1-1.el7.x86\_64 util-linux-2.23.2-65.el7\_9.1.x86\_64 acl-2.2.51-15.el7.x86\_64 device-mapper-1.02.170-6.el7\_9.5.x86\_64 tar-1.26-35.el7.x86\_64 device-mapper-event-libs-1.02.170-6.el7\_9.5.x86\_64 libdb-utils-5.3.21-25.el7.x86\_64 initscripts-9.49.53-1.el7\_9.1.x86\_64 libss-1.42.9-19.el7.x86\_64 grub2-pc-2.02-0.87.el7.centos.6.x86\_64 make-3.82-24.el7.x86\_64 lvm2-libs-2.02.187-6.el7\_9.5.x86\_64 kernel-tools-libs-3.10.0-1160.42.2.el7.x86\_64 linux-firmware-20200421-80.git78c0348.el7\_9.noarch mozjs17-17.0.0-20.el7.x86\_64 firewalld-0.6.3-13.el7\_9.noarch snappy-1.1.0-3.el7.x86\_64 tuned-2.11.0-11.el7\_9.noarch libndp-1.2-9.el7.x86\_64 grub2-2.02-0.87.el7.centos.6.x86\_64 ustr-1.0.4-16.el7.x86\_64 kpartx-0.4.9-135.el7\_9.x86\_64 libtasn1-4.10-1.el7.x86\_64 selinux-policy-targeted-3.13.1-268.el7\_9.2.noarch NetworkManager-team-1.18.8-2.el7\_9.x86\_64 krb5-libs-1.15.1-50.el7.x86\_64 rsyslog-8.24.0-57.el7\_9.1.x86\_64 kexec-tools-2.0.15-51.el7\_9.3.x86\_64 libcroco-0.6.12-6.el7\_9.x86\_64 gzip-1.5-10.el7.x86\_64 iprutils-2.4.17.1-3.el7\_7.x86\_64 python-decorator-3.4.0-3.el7.noarch iwl2030-firmware-18.168.6.1-80.el7\_9.noarch iwl135-firmware-18.168.6.1-80.el7\_9.noarch iwl5150-firmware-8.24.2.2-80.el7\_9.noarch pam-1.1.8-23.el7.x86\_64 cyrus-sasl-lib-2.1.26-23.el7.x86\_64 gettext-0.19.8.1-3.el7.x86\_64 yum-metadata-parser-1.1.4-10.el7.x86\_64 python-gobject-base-3.22.0-1.el7\_4.1.x86\_64 python-iniparse-0.4-9.el7.noarch newt-python-0.52.15-4.el7.x86\_64 python-linux-procfs-0.4.11-4.el7.noarch python-slip-0.4.0-4.el7.noarch grubby-8.28-26.el7.x86\_64 libssh2-1.8.0-4.el7.x86\_64 fipscheck-lib-1.4.1-6.el7.x86\_64 rpm-4.11.3-45.el7.x86\_64 libuser-0.60-9.el7.x86\_64 python-urlgrabber-3.10-10.el7.noarch centos-logos-70.0.6-3.el7.centos.noarch logrotate-3.8.6-19.el7.x86\_64 libfastjson-0.99.4-3.el7.x86\_64 qrencode-libs-3.4.1-3.el7.x86\_64 libpipeline-1.2.3-3.el7.x86\_64 lsscsi-0.27-6.el7.x86\_64 numactl-libs-2.0.12-5.el7.x86\_64 cryptsetup-libs-2.0.3-6.el7.x86\_64 kmod-20-28.el7.x86\_64 elfutils-default-yama-scope-0.176-5.el7.noarch polkit-pkla-compat-0.1-4.el7.x86\_64 policycoreutils-2.5-34.el7.x86\_64 os-prober-1.58-9.el7.x86\_64 cronie-anacron-1.4.11-23.el7.x86\_64 crontabs-1.11-6.20121102git.el7.noarch openssh-7.4p1-21.el7.x86\_64 fxload-2002\_04\_11-16.el7.x86\_64 alsa-tools-firmware-1.1.0-1.el7.x86\_64 libpciaccess-0.14-1.el7.x86\_64 teamd-1.29-3.el7.x86\_64 dbus-python-1.1.1-9.el7.x86\_64 plymouth-scripts-0.8.9-0.34.20140113.el7.centos.x86\_64 python-pyudev-0.15-9.el7.noarch pth-2.0.7-23.el7.x86\_64 rpm-build-libs-4.11.3-45.el7.x86\_64 gpgme-1.3.2-5.el7.x86\_64 yum-plugin-fastestmirror-1.1.31-54.el7\_8.noarch kbd-misc-1.15.5-15.el7.noarch iwl105-firmware-18.168.6.1-80.el7\_9.noarch iwl4965-firmware-228.61.2.24-80.el7\_9.noarch iwl6000g2b-firmware-18.168.6.1-80.el7\_9.noarch iwl100-firmware-39.31.5.1-80.el7\_9.noarch iwl6000-firmware-9.221.4.1-80.el7\_9.noarch basesystem-10.0-7.el7.centos.noarch postfix-2.10.1-9.el7.x86\_64 aic94xx-firmware-30-6.el7.noarch dracut-config-rescue-033-572.el7.x86\_64 bash-4.2.46-34.el7.x86\_64 passwd-0.79-6.el7.x86\_64 e2fsprogs-1.42.9-19.el7.x86\_64 chkconfig-1.7.6-1.el7.x86\_64 gawk-4.0.2-4.el7\_3.1.x86\_64 libcap-2.22-11.el7.x86\_64 libffi-3.0.13-19.el7.x86\_64 expat-2.1.0-12.el7.x86\_64 grub2-pc-modules-2.02-0.87.el7.centos.6.noarch diffutils-3.3-5.el7.x86\_64 glibc-2.17-324.el7\_9.x86\_64 file-5.11-37.el7.x86\_64 systemd-libs-219-78.el7\_9.3.x86\_64 libnl3-cli-3.2.28-4.el7.x86\_64 libblkid-2.23.2-65.el7\_9.1.x86\_64 e2fsprogs-libs-1.42.9-19.el7.x86\_64 python-2.7.5-90.el7.x86\_64 libidn-1.28-4.el7.x86\_64 NetworkManager-libnm-1.18.8-2.el7\_9.x86\_64 sysvinit-tools-2.88-14.dsf.el7.x86\_64 systemd-219-78.el7\_9.3.x86\_64 gdbm-1.10-8.el7.x86\_64 wpa\_supplicant-2.6-12.el7\_9.2.x86\_64 pciutils-libs-3.5.1-3.el7.x86\_64 selinux-policy-3.13.1-268.el7\_9.2.noarch iptables-1.4.21-35.el7.x86\_64 device-mapper-persistent-data-0.8.5-3.el7\_9.2.x86\_64 device-mapper-libs-1.02.170-6.el7\_9.5.x86\_64 grub2-tools-2.02-0.87.el7.centos.6.x86\_64 pinentry-0.8.1-17.el7.x86\_64 device-mapper-event-1.02.170-6.el7\_9.5.x86\_64 libpng-1.5.13-8.el7.x86\_64 firewalld-filesystem-0.6.3-13.el7\_9.noarch ncurses-5.9-14.20130511.el7\_4.x86\_64 kernel-tools-3.10.0-1160.42.2.el7.x86\_64 dhclient-4.2.5-83.el7.centos.1.x86\_64 libsemanage-2.5-14.el7.x86\_64 NetworkManager-tui-1.18.8-2.el7\_9.x86\_64 microcode\_ctl-2.1-73.11.el7\_9.x86\_64 openssl-1.0.2k-21.el7\_9.x86\_64 cracklib-2.9.0-11.el7.x86\_64 iwl6050-firmware-41.28.5.1-80.el7\_9.noarch shared-mime-info-1.8-5.el7.x86\_64 iwl7260-firmware-25.30.13.0-80.el7\_9.noarch libpwquality-1.2.3-5.el7.x86\_64 iwl1000-firmware-39.31.5.1-80.el7\_9.noarch pkgconfig-0.27.1-4.el7.x86\_64 iwl3160-firmware-25.30.13.0-80.el7\_9.noarch libutempter-1.1.6-4.el7.x86\_64 python-schedutils-0.4-6.el7.x86\_64 libselinux-python-2.5-15.el7.x86\_64 mariadb-libs-5.5.68-1.el7.x86\_64 fipscheck-1.4.1-6.el7.x86\_64 rpm-libs-4.11.3-45.el7.x86\_64 python-pycurl-7.19.0-19.el7.x86\_64 alsa-lib-1.1.8-1.el7.x86\_64 libdaemon-0.14-7.el7.x86\_64 libestr-0.1.9-2.el7.x86\_64 json-c-0.11-4.el7\_0.x86\_64 dracut-033-572.el7.x86\_64 dbus-libs-1.10.24-15.el7.x86\_64 polkit-0.112-26.el7.x86\_64 cronie-1.4.11-23.el7.x86\_64 dracut-network-033-572.el7.x86\_64 alsa-firmware-1.0.28-2.el7.noarch libdrm-2.4.97-2.el7.x86\_64 python-slip-dbus-0.4.0-4.el7.noarch plymouth-0.8.9-0.34.20140113.el7.centos.x86\_64 gnupg2-2.0.22-5.el7\_5.x86\_64 pygpgme-0.3-9.el7.x86\_64 |
| **查看主机名** | hostname |
| **检查结果** | localhost.localdomain |
| **查看网络配置** | ifconfig -a |
| **检查结果** |  |
| **查看路由表** | netstat -rn |
| **检查结果** |  |
| **查看开放端口** | netstat -an |
| **检查结果** |  |
| **查看当前进程** | ps -aux |
| **检查结果** | USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 1 0.0 0.3 128024 6636 ? Ss 10:19 0:01 /usr/lib/systemd/systemd --switched-root --system --deserialize 22 root 2 0.0 0.0 0 0 ? S 10:19 0:00 [kthreadd] root 4 0.0 0.0 0 0 ? S< 10:19 0:00 [kworker/0:0H] root 5 0.0 0.0 0 0 ? S 10:19 0:00 [kworker/u256:0] root 6 0.0 0.0 0 0 ? S 10:19 0:01 [ksoftirqd/0] root 7 0.0 0.0 0 0 ? S 10:19 0:00 [migration/0] root 8 0.0 0.0 0 0 ? S 10:19 0:00 [rcu\_bh] root 9 0.0 0.0 0 0 ? S 10:19 0:05 [rcu\_sched] root 10 0.0 0.0 0 0 ? S< 10:19 0:00 [lru-add-drain] root 11 0.0 0.0 0 0 ? S 10:19 0:00 [watchdog/0] root 12 0.0 0.0 0 0 ? S 10:19 0:00 [watchdog/1] root 13 0.0 0.0 0 0 ? S 10:19 0:00 [migration/1] root 14 0.0 0.0 0 0 ? S 10:19 0:02 [ksoftirqd/1] root 16 0.0 0.0 0 0 ? S< 10:19 0:00 [kworker/1:0H] root 18 0.0 0.0 0 0 ? S 10:19 0:00 [kdevtmpfs] root 19 0.0 0.0 0 0 ? S< 10:19 0:00 [netns] root 20 0.0 0.0 0 0 ? S 10:19 0:00 [khungtaskd] root 21 0.0 0.0 0 0 ? S< 10:19 0:00 [writeback] root 22 0.0 0.0 0 0 ? S< 10:19 0:00 [kintegrityd] root 23 0.0 0.0 0 0 ? S< 10:19 0:00 [bioset] root 24 0.0 0.0 0 0 ? S< 10:19 0:00 [bioset] root 25 0.0 0.0 0 0 ? S< 10:19 0:00 [bioset] root 26 0.0 0.0 0 0 ? S< 10:19 0:00 [kblockd] root 27 0.0 0.0 0 0 ? S< 10:19 0:00 [md] root 28 0.0 0.0 0 0 ? S< 10:19 0:00 [edac-poller] root 29 0.0 0.0 0 0 ? S< 10:19 0:00 [watchdogd] root 30 0.0 0.0 0 0 ? S 10:19 0:04 [kworker/0:1] root 35 0.0 0.0 0 0 ? S 10:19 0:00 [kswapd0] root 36 0.0 0.0 0 0 ? SN 10:19 0:00 [ksmd] root 37 0.0 0.0 0 0 ? SN 10:19 0:00 [khugepaged] root 38 0.0 0.0 0 0 ? S< 10:19 0:00 [crypto] root 46 0.0 0.0 0 0 ? S< 10:19 0:00 [kthrotld] root 48 0.0 0.0 0 0 ? S< 10:19 0:00 [kmpath\_rdacd] root 49 0.0 0.0 0 0 ? S< 10:19 0:00 [kaluad] root 50 0.0 0.0 0 0 ? S< 10:19 0:00 [kpsmoused] root 51 0.0 0.0 0 0 ? S 10:19 0:00 [kworker/0:2] root 52 0.0 0.0 0 0 ? S< 10:19 0:00 [ipv6\_addrconf] root 65 0.0 0.0 0 0 ? S< 10:19 0:00 [deferwq] root 101 0.0 0.0 0 0 ? S 10:19 0:00 [kauditd] root 283 0.0 0.0 0 0 ? S< 10:19 0:00 [nfit] root 284 0.0 0.0 0 0 ? S< 10:19 0:00 [mpt\_poll\_0] root 285 0.0 0.0 0 0 ? S< 10:19 0:00 [mpt/0] root 286 0.0 0.0 0 0 ? S< 10:19 0:00 [ata\_sff] root 294 0.0 0.0 0 0 ? S 10:19 0:00 [scsi\_eh\_0] root 295 0.0 0.0 0 0 ? S< 10:19 0:00 [scsi\_tmf\_0] root 296 0.0 0.0 0 0 ? S 10:19 0:00 [scsi\_eh\_1] root 298 0.0 0.0 0 0 ? S< 10:19 0:00 [scsi\_tmf\_1] root 299 0.0 0.0 0 0 ? S 10:19 0:00 [scsi\_eh\_2] root 300 0.0 0.0 0 0 ? S< 10:19 0:00 [scsi\_tmf\_2] root 303 0.0 0.0 0 0 ? S 10:19 0:00 [irq/16-vmwgfx] root 304 0.0 0.0 0 0 ? S< 10:19 0:00 [ttm\_swap] root 374 0.0 0.0 0 0 ? S< 10:19 0:00 [kdmflush] root 375 0.0 0.0 0 0 ? S< 10:19 0:00 [bioset] root 385 0.0 0.0 0 0 ? S< 10:19 0:00 [kdmflush] root 386 0.0 0.0 0 0 ? S< 10:19 0:00 [bioset] root 398 0.0 0.0 0 0 ? S< 10:19 0:00 [bioset] root 399 0.0 0.0 0 0 ? S< 10:19 0:00 [xfsalloc] root 400 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs\_mru\_cache] root 401 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-buf/dm-0] root 402 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-data/dm-0] root 403 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-conv/dm-0] root 404 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-cil/dm-0] root 405 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-reclaim/dm-] root 406 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-log/dm-0] root 407 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-eofblocks/d] root 408 0.0 0.0 0 0 ? S 10:19 0:03 [xfsaild/dm-0] root 409 0.0 0.0 0 0 ? S< 10:19 0:00 [kworker/0:1H] root 487 0.0 0.1 39056 3092 ? Ss 10:19 0:00 /usr/lib/systemd/systemd-journald root 506 0.0 0.2 201104 4136 ? Ss 10:19 0:00 /usr/sbin/lvmetad -f root 517 0.0 0.3 49552 6032 ? Ss 10:19 0:00 /usr/lib/systemd/systemd-udevd root 553 0.0 0.0 0 0 ? S< 10:19 0:00 [kdmflush] root 554 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-buf/sda1] root 555 0.0 0.0 0 0 ? S< 10:19 0:00 [bioset] root 556 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-data/sda1] root 557 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-conv/sda1] root 558 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-cil/sda1] root 560 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-reclaim/sda] root 561 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-log/sda1] root 562 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-eofblocks/s] root 565 0.0 0.0 0 0 ? S 10:19 0:00 [xfsaild/sda1] root 587 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-buf/dm-2] root 589 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-data/dm-2] root 590 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-conv/dm-2] root 606 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-cil/dm-2] root 614 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-reclaim/dm-] root 616 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-log/dm-2] root 617 0.0 0.0 0 0 ? S< 10:19 0:00 [xfs-eofblocks/d] root 618 0.0 0.0 0 0 ? S 10:19 0:00 [xfsaild/dm-2] root 642 0.0 0.0 55532 1080 ? S<sl 10:19 0:02 /sbin/auditd dbus 664 0.0 0.1 66448 2588 ? Ssl 10:19 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation root 668 0.0 0.0 21684 1304 ? Ss 10:19 0:00 /usr/sbin/irqbalance --foreground polkitd 669 0.0 0.6 613024 12996 ? Ssl 10:19 0:00 /usr/lib/polkit-1/polkitd --no-debug root 671 0.0 0.0 26384 1780 ? Ss 10:19 0:00 /usr/lib/systemd/systemd-logind root 674 0.0 0.0 126388 1668 ? Ss 10:19 0:00 /usr/sbin/crond -n root 679 0.0 0.1 96572 2456 ? Ss 10:19 0:00 login -- root chrony 681 0.0 0.0 117808 1856 ? S 10:19 0:00 /usr/sbin/chronyd root 696 0.0 1.5 359104 29760 ? Ssl 10:19 0:00 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid root 697 0.0 0.6 702464 11332 ? Ssl 10:19 0:00 /usr/sbin/NetworkManager --no-daemon root 823 0.0 0.2 102944 5520 ? S 10:19 0:00 /sbin/dhclient -d -q -sf /usr/libexec/nm-dhcp-helper -pf /var/run/dhclient-ens33.pid -lf /var/lib/NetworkManager/dhclient-57d4a5e5-0fce-3895-acf4-743d9cbe8f7a-ens33.lease -cf /var/lib/NetworkManager/dhclient-ens33.conf ens33 root 992 0.0 0.2 112940 4348 ? Ss 10:19 0:00 /usr/sbin/sshd -D root 994 0.0 0.9 574288 17464 ? Ssl 10:19 0:01 /usr/bin/python2 -Es /usr/sbin/tuned -l -P root 995 0.0 0.2 216400 4664 ? Ssl 10:19 0:00 /usr/sbin/rsyslogd -n root 1032 0.0 0.0 0 0 ? S< 10:19 0:00 [kworker/1:1H] root 1306 0.0 0.1 89748 2140 ? Ss 10:19 0:00 /usr/libexec/postfix/master -w postfix 1315 0.0 0.2 89920 4100 ? S 10:19 0:00 qmgr -l -t unix -u root 8190 0.0 0.1 115544 2040 tty1 Ss+ 10:19 0:00 -bash root 8210 0.6 0.3 159260 6036 ? Ss 10:20 0:40 sshd: root@pts/0,pts/1 root 8214 0.0 0.1 115548 2096 pts/0 Ss 10:20 0:00 -bash root 8227 0.0 0.3 158944 5612 ? Ss 10:20 0:00 sshd: root@notty root 8228 0.0 0.1 115548 1988 pts/1 Ss 10:20 0:00 -bash root 8244 0.0 0.1 72292 2864 ? Ss 10:20 0:00 /usr/libexec/openssh/sftp-server root 8249 0.0 0.1 72292 2688 ? Ss 10:20 0:00 /usr/libexec/openssh/sftp-server root 8254 0.0 0.1 72292 2688 ? Ss 10:20 0:00 /usr/libexec/openssh/sftp-server root 8259 0.0 0.1 72292 2692 ? Ss 10:20 0:00 /usr/libexec/openssh/sftp-server root 8264 0.0 0.1 72292 2688 ? Ss 10:20 0:00 /usr/libexec/openssh/sftp-server root 8269 0.0 0.1 72292 2692 ? Ss 10:20 0:00 /usr/libexec/openssh/sftp-server root 8322 0.1 0.1 162816 3060 pts/1 S+ 10:20 0:08 top root 12396 0.0 0.0 0 0 ? S 10:24 0:00 [kworker/u256:1] root 102929 0.0 0.0 0 0 ? S 11:52 0:00 [kworker/1:2] postfix 108839 0.0 0.2 89852 4080 ? S 11:59 0:00 pickup -l -t unix -u root 112671 0.0 0.0 0 0 ? S 12:03 0:00 [kworker/1:1] root 117734 0.0 0.0 0 0 ? S 12:09 0:00 [kworker/1:0] root 120216 1.0 0.3 158944 5616 ? Ss 12:11 0:00 sshd: root@notty root 120222 0.0 0.1 72292 2684 ? Ss 12:11 0:00 /usr/libexec/openssh/sftp-server root 120233 0.0 0.1 72292 2684 ? Ss 12:11 0:00 /usr/libexec/openssh/sftp-server root 120241 0.0 0.1 72292 2688 ? Ss 12:11 0:00 /usr/libexec/openssh/sftp-server root 120246 0.0 0.1 72292 2688 ? Ss 12:11 0:00 /usr/libexec/openssh/sftp-server root 120251 0.0 0.1 72292 2688 ? Ss 12:11 0:00 /usr/libexec/openssh/sftp-server root 120256 0.0 0.1 72292 2688 ? Ss 12:11 0:00 /usr/libexec/openssh/sftp-server root 120420 0.0 0.0 115348 1592 ? Ss 12:11 0:00 bash -c export LANG="en\_US";export LANGUAGE="en\_US";export LC\_ALL="en\_US";free;echo finalshell\_separator;uptime;echo finalshell\_separator;cat /proc/net/dev;echo finalshell\_separator;df;echo finalshell\_separator;sleep 1;free;echo finalshell\_separator;uptime;echo finalshell\_separator;cat /proc/net/dev;echo finalshell\_separator;df;echo finalshell\_separator; root 120427 0.0 0.0 108056 356 ? S 12:11 0:00 sleep 1 root 120428 0.0 0.0 115616 1248 pts/0 S+ 12:11 0:00 -bash root 120449 0.0 0.0 115616 880 pts/0 S+ 12:11 0:00 -bash root 120450 0.0 0.0 155452 1860 pts/0 R+ 12:11 0:00 ps -aux |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **系统 core dump 状态**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-02-02-01** |
| **操作目的** | 限制系统core dump信息输出，防止系统信息暴露 |
| **检查方法** | 执行more /etc/security/limits.conf， 检查是否包含下列  项：  \* soft core 0  \* hard core 0 |
| **检查结果** | 是否符合：  不适用  现状：  # /etc/security/limits.conf # #This file sets the resource limits for the users logged in via PAM. #It does not affect resource limits of the system services. # #Also note that configuration files in /etc/security/limits.d directory, #which are read in alphabetical order, override the settings in this #file in case the domain is the same or more specific. #That means for example that setting a limit for wildcard domain here #can be overriden with a wildcard setting in a config file in the #subdirectory, but a user specific setting here can be overriden only #with a user specific setting in the subdirectory. # #Each line describes a limit for a user in the form: # #<domain> <type> <item> <value> # #Where: #<domain> can be: # - a user name # - a group name, with @group syntax # - the wildcard \*, for default entry # - the wildcard %, can be also used with %group syntax, # for maxlogin limit # #<type> can have the two values: # - "soft" for enforcing the soft limits # - "hard" for enforcing hard limits # #<item> can be one of the following: # - core - limits the core file size (KB) # - data - max data size (KB) # - fsize - maximum filesize (KB) # - memlock - max locked-in-memory address space (KB) # - nofile - max number of open file descriptors # - rss - max resident set size (KB) # - stack - max stack size (KB) # - cpu - max CPU time (MIN) # - nproc - max number of processes # - as - address space limit (KB) # - maxlogins - max number of logins for this user # - maxsyslogins - max number of logins on the system # - priority - the priority to run user process with # - locks - max number of file locks the user can hold # - sigpending - max number of pending signals # - msgqueue - max memory used by POSIX message queues (bytes) # - nice - max nice priority allowed to raise to values: [-20, 19] # - rtprio - max realtime priority # #<domain> <type> <item> <value> #  #\* soft core 0 #\* hard rss 10000 #@student hard nproc 20 #@faculty soft nproc 20 #@faculty hard nproc 50 #ftp hard nproc 0 #@student - maxlogins 4  # End of file |
| **加固方法** | 备份：  cp /etc/security/limits.conf /etc/security/limits.conf.bak20210603  执行vim /etc/security/limits.conf  若配置文件中没有限制，则增加如下如下两行：  \* soft core 0  \* hard core 0 |
| **加固结果** | 未加固 |
| **回退方法** | cp /etc/security/limits.conf.bak20210603 /etc/security/limits.conf  则可回退 |
| **基线符合性**  **判定依据** | 若不存在，则低于安全要求 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | core dump 中会输出很多系统信息，易被入侵者利用。 |

* + 1. **账号**
       1. **检查弱口令**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-01-01** |
| **操作目的** | 检查弱口令，防止口令被暴力破解 |
| **检查方法** | 1、将被检查主机的/etc/shadow文件拷贝到安全检查工程师终端；  2、在终端上执行john the ripper工具（密码工具）以检测弱口令：  john.exe 'shadow' –single  或者，使用pass.txt字典（密码工具）检查弱口令：  john.exe 'shadow' --wordlist='pass.txt' |
| **检查结果** | 是否符合：  符合  现状：  经询问无弱口令 |
| **加固方法** | 使用“passwd 用户名”命令为所有用户设置复杂密码 |
| **加固结果** | 未加固 |
| **回退方法** | 不需要回退 |
| **基线符合性**  **判定依据** | 密码安全策略要求为密码不包含用户名；密码长度大于等于12位；必须同时包含字母、数字和特殊字符中两者；密码最长使用天数不超过90天。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | John.exe外部弱口令检测工具，下载地址：  https://www.techspot.com/downloads/6970-john-the-ripper.html |

* + - 1. **禁用无用账号**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-02-01** |
| **操作目的** | 禁用系统无用账号，防止恶意人员通过无用账号非授权进入系统 |
| **检查方法** | 与系统管理员确认不必要的账号，如FTP等服务账号；  执行“cat /etc/passwd”，查看ftp账号shell是否为/sbin/nologin：    执行“cat /etc/shadow”,查看ftp是否被锁定：    被锁定账户的加密字段（第二个字段）前面会有!或者\*。 |
| **检查结果** | 是否符合：  符合  现状：  root:/bin/bash bin:/sbin/nologin daemon:/sbin/nologin adm:/sbin/nologin lp:/sbin/nologin sync:/bin/sync shutdown:/sbin/shutdown halt:/sbin/halt mail:/sbin/nologin operator:/sbin/nologin games:/sbin/nologin ftp:/sbin/nologin nobody:/sbin/nologin systemd-network:/sbin/nologin dbus:/sbin/nologin polkitd:/sbin/nologin sshd:/sbin/nologin postfix:/sbin/nologin chrony:/sbin/nologin |
| **加固方法** | 使用命令“passwd -l <用户名>或者 userdel <用户名>”锁定或删除不必要的账号。  passwd -l adm  passwd -l lp  passwd -l sync  passwd -l shutdown  passwd -l halt  passwd -l news  passwd -l uucp  passwd -l operator  passwd -l games  passwd -l gopher  passwd -l ftp |
| **加固结果** | 未加固 |
| **回退方法** | 使用命令“passwd -u <用户名>”解锁账号 |
| **基线符合性**  **判定依据** | 锁定或删除adm、lp、sync、shutdown、halt、news、uucp、operator、games、gopher、ftp等用户，以及与用户确确认的其他无用账号； |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 必须与管理员确认锁定或删除的用户为无用用户，不影响业务正常运行。 |

* + - 1. **账号锁定策略**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-03-01** |
| **操作目的** | 限制登录尝试错误次数和设置账号锁定时间，防止口令暴力破解。 |
| **检查方法** | 执行“cat /etc/pam.d/system-auth”命令，查看是否如下配置：  auth required pam\_tally2.so deny=10 unlock\_time =300 even\_deny\_root root\_unlock\_time=300  deny：设置普通用户和root用户连续错误登陆的最大次数，超过最大次数，则锁定该用户；  unlock\_time：设定普通用户锁定后，多少时间后解锁，单位是秒；  even\_deny\_root：限制root用户；  root\_unlock\_time ：设定root用户锁定后，多少时间后解锁，单位是秒； |
| **检查结果** | 是否符合：  不符合  现状：  #%PAM-1.0 # This file is auto-generated. # User changes will be destroyed the next time authconfig is run. auth required pam\_env.so auth required pam\_faildelay.so delay=2000000 auth sufficient pam\_unix.so nullok try\_first\_pass auth requisite pam\_succeed\_if.so uid >= 1000 quiet\_success auth required pam\_deny.so  account required pam\_unix.so account sufficient pam\_localuser.so account sufficient pam\_succeed\_if.so uid < 1000 quiet account required pam\_permit.so  password requisite pam\_pwquality.so try\_first\_pass local\_users\_only retry=3 authtok\_type= password sufficient pam\_unix.so sha512 shadow nullok try\_first\_pass use\_authtok password required pam\_deny.so  session optional pam\_keyinit.so revoke session required pam\_limits.so -session optional pam\_systemd.so session [success=1 default=ignore] pam\_succeed\_if.so service in crond quiet use\_uid session required pam\_unix.so |
| **加固方法** | 备份配置文件：  cp /etc/pam.d/system-auth /etc/pam.d/system-auth.bak  设置连续输错10次密码，帐号锁定5分钟：  使用命令“vim /etc/pam.d/system-auth”修改配置文件，添加：  auth required pam\_tally2.so deny=10 unlock\_time =300 even\_deny\_root root\_unlock\_time=300 |
| **加固结果** | 未加固 |
| **回退方法** | cp /etc/pam.d/system-auth.bak /etc/pam.d/system-auth |
| **基线符合性**  **判定依据** | 连续输入错误口令10次系统账号锁定，锁定时间5分钟后自动解锁，可继续登录系统。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 防止暴力破解 |

* + - 1. **检查空口令账户和除 root 外 UID 为 0 的用户**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-04-01** |
| **操作目的** | 查看空口令和root权限的账号 |
| **检查方法** | 使用命令“awk -F: '($2=="")' /etc/shadow”查看空口令账号  使用命令“awk -F: '($3==0)' /etc/passwd”查看UID为0的账号 |
| **检查结果** | 是否符合：  符合  现状：  root:x:0:0:root:/root:/bin/bash |
| **加固方法** | 备份文件：  cp /etc/passwd /etc/passwd.bak  cp /etc/shadow /etc/shadow.bak  使用命令“passwd <用户名>”为空口令账号设定密码；  UID为0的账号应该只有root，设置UID方法：  usermod -u UID <用户名> |
| **加固结果** | 未加固 |
| **回退方法** | cp /etc/passwd.bak /etc/passwd  cp /etc/shadow.bak /etc/ shadow |
| **基线符合性**  **判定依据** | 不存在空口令账号；只有root用户的UID为0。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **添加口令周期策略**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-05-01** |
| **操作目的** | 设置口令使用周期，防止口令长时间使用，降低口令泄露风险。 |
| **检查方法** | 使用命令“cat /etc/login.defs|grep PASS”查看密码策略设置：  PASS\_MAX\_DAYS 90 #新建用户的密码最长使用天数  PASS\_MIN\_DAYS 0 #新建用户的密码最短使用天数  PASS\_MIN\_LAN 12 #新建用户的密码最短使用天数PASS\_WARN\_AGE 7 #新建用户的密码到期提前提醒天数  最小位数 min len |
| **检查结果** | 是否符合：  不符合  现状：  # PASS\_MAX\_DAYS Maximum number of days a password may be used. # PASS\_MIN\_DAYS Minimum number of days allowed between password changes. # PASS\_MIN\_LEN Minimum acceptable password length. # PASS\_WARN\_AGE Number of days warning given before a password expires. PASS\_MAX\_DAYS 99999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LEN 5 PASS\_WARN\_AGE 7 |
| **加固方法** | 拷贝文件“cp /etc/login.defs /etc/login.defs.bak”  使用命令“vim /etc/login.defs”修改配置文件  PASS\_MAX\_DAYS 90 #新建用户的密码最长使用天数  PASS\_MIN\_DAYS 0 #新建用户的密码最短使用天数  PASS\_MIN\_LAN 12 #新建用户的密码最短使用天数PASS\_WARN\_AGE 7 #新建用户的密码到期提前提醒天数  或者使用chage命令修改特定用户设置，例如：  chage -m 0 -M 90 -E 2020-05-31 -W 7 <用户名>  表示：将此用户的密码最长使用天数设为90，最短使用天数设为0，帐号2020年5月31日过期，过期前7天里警告用户。 |
| **加固结果** | 未加固 |
| **回退方法** | vim /etc/login.defs将相关加固配置改回原来的值 |
| **基线符合性**  **判定依据** | 用户密码最长使用天数90天，最短使用天数0天，账号过期前7天里提醒用户。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **添加口令复杂度策略**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-06-01** |
| **操作目的** | 加强口令的复杂度要求，防止弱口令，降低被暴力破解的可能性 |
| **检查方法** | 使用命令“cat /etc/pam.d/system-auth |grep pam\_cracklib.so”查看密码复杂度策略设置：  password requisite pam\_cracklib.so difok=3 minlen=12 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minclass=2  difok=3 #新密码与旧密码不同的字符个数为3个  minlen=12 #密码长度至少12位  ucredit=-1 #至少1个大写  lcredit=-1 #至少1个小写  dcredit=-1 #至少1个数字  ocredit=-1 #至少1个特殊字符  minclass=2 #四种类型字符中至少两种组合 |
| **检查结果** | 是否符合：  不符合  现状： |
| **加固方法** | 拷贝文件“cp /etc/pam.d/system-auth /etc/pam.d/system-auth.bak”  修改“vim /etc/pam.d/system-auth”文件中配置为：  password requisite pam\_cracklib.so difok=3 minlen=12 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 minclass=2 |
| **加固结果** | 未加固 |
| **回退方法** | 还原备份文件。 |
| **基线符合性**  **判定依据** | 测试修改特定用户口令；口令满足要求为：至少12位，大写字母、小写字母、数字、特殊字符至少2类组成，新旧密码至少3个字符不同。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **限制root远程登录**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-07-01** |
| **操作目的** | 限制root远程telnet登录，如果禁止telnet服务可忽略此项 |
| **检查方法** | 使用命令“cat /etc/securetty |grep console”查看是否禁止root远程登录  console=/dev/tty01 |
| **检查结果** | 是否符合：  不符合  现状：  console |
| **加固方法** | vim /etc/securetty编辑文件，配置：  console=/dev/tty01 |
| **加固结果** | 未加固 |
| **回退方法** | vim /etc/securetty编辑文件，配置：  #console=/dev/tty01 |
| **基线符合性**  **判定依据** | root帐户不能远程telnet登录系统 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 若禁止telnet服务，则可忽略此配置 |

* + - 1. **检查Grub密码**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-08-01** |
| **操作目的** | 查看系统引导管理器是否设置密码，确保系统引导安全。 |
| **检查方法** | 使用命令 “cat /boot/grub2/grub.cfg|grep password”  替换  使用命令 “cat /boot/grub2/grub.cfg|grep password”或“cat /boot/efi/EFI/centos/grub.cfg |grep password”，  然后在“cat /boot/grub2/user.cfg”文件  替换  然后在“cat /boot/grub2/user.cfg”文件或者“cat /boot/efi/EFI/centos/user.cfg” |
| **检查结果** | 是否符合：  不符合  现状：  if [ -n "${GRUB2\_PASSWORD}" ]; then  password\_pbkdf2 root ${GRUB2\_PASSWORD} |
| **加固方法** | vim /boot/grub/grub.conf打开配置文件；  在hiddenmenu行下方增加一行：  “password 明文密码”或者“password -md5 md5方式密码”，如下所示：  这里写图片描述  如果采用md5方式密码，则需要提前生成md5密码：    （CentOS 6、RedHat 6）。  执行命令grub2-setpassword，输入密码和确认密码。  然后在/boot/grub2/user.cfg文件中出现密码即可    （CentOS 7、RedHat 7）。 |
| **加固结果** | 未加固 |
| **回退方法** | 去掉增加的密码行（CentOS 6、RedHat 6）。  删除文件中的password bengang  清除/boot/grub2/user.cfg文件中的密码（CentOS 7、RedHat 7）。 |
| **基线符合性**  **判定依据** | 启动系统进行系统引导阶段时进入grub菜单提示输入密码。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 此配置对技术能力要求较高，配置不当将导致系统无法启动。 |

* + - 1. **限制用户su**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-09-01** |
| **操作目的** | 限制能su到root的普通用户，只允许特定的用户组可以su root。 |
| **检查方法** | 使用命令“cat /etc/pam.d/su”,查看是否有  “auth required/lib/security/pam\_wheel.so”这样的配置条目 |
| **检查结果** | 是否符合：  不符合  现状：  #%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 # Uncomment the following line to require a user to be in the "wheel" group. #auth required pam\_wheel.so use\_uid auth substack system-auth auth include postlogin account sufficient pam\_succeed\_if.so uid = 0 use\_uid quiet account include system-auth password include system-auth session include system-auth session include postlogin session optional pam\_xauth.so |
| **加固方法** | 使用命令“vim /etc/pam.d/su”文件中增加条目：  “auth required pam\_wheel.so group=wheel ”  只允许wheel组的用户可以su到root，如下：  然后通过“usermod -g wheel 用户名”，将允许su root的用户添加到wheel组。  举例：将test用户加入到wheel组，使用命令“usermod -g wheel test”。 |
| **加固结果** | 未加固 |
| **回退方法** | 注释掉auth required pam\_wheel.so group=wheel |
| **基线符合性**  **判定依据** | 只允许wheel组的用户可以通过su到root。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 不清楚业务用户需求，暂未进行限制 |

* + - 1. **SNMP团体字**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-03-10-01** |
| **操作目的** | 修改snmp默认团体字，确保snmp服务安全 |
| **检查方法** | 使用命令“cat /etc/snmp/snmpd.conf” |
| **检查结果** | 是否符合：  不适用  现状：  没找到配置文件 |
| **加固方法** | vim /etc/snmp/snmpd.conf打开配置文件；  将“com2sec notConfigUser default public”的默认团体字“public”改成自定义的安全的团队字，如“2020@Password!”。 |
| **加固结果** | 未加固 |
| **回退方法** | 将“2020@Password!”改回“public” |
| **基线符合性**  **判定依据** | Snmp团体字不是默认的团体字，采用了安全的自定义的团体字。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 若无必要SNMP服务，应禁止使用snmp服务。 |

* + 1. **服务**
       1. **关闭不必要的服务**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-04-01-01** |
| **操作目的** | 关闭不必要的服务，提供系统性能，降低开放服务风险 |
| **检查方法** | 使用命令“who -r”查看当前init级别    使用命令“chkconfig --list ”查看chkconfig设置的所有服务的状态    使用命令“systemctl list-unit-files | grep enable”查看所有通过systemctl设置的随系统启动服务 |
| **检查结果** | 是否符合：  符合，高危telnet协议未开启。  现状：  auditd.service enabled  autovt@.service enabled  chronyd.service enabled  crond.service enabled  dbus-org.fedoraproject.FirewallD1.service enabled  dbus-org.freedesktop.nm-dispatcher.service enabled  firewalld.service enabled  getty@.service enabled  irqbalance.service enabled  kdump.service enabled  lvm2-monitor.service enabled  microcode.service enabled  NetworkManager-dispatcher.service enabled  NetworkManager-wait-online.service enabled  NetworkManager.service enabled  postfix.service enabled  rhel-autorelabel-mark.service enabled  rhel-autorelabel.service enabled  rhel-configure.service enabled  rhel-dmesg.service enabled  rhel-domainname.service enabled  rhel-import-state.service enabled  rhel-loadmodules.service enabled  rhel-readonly.service enabled  rsyslog.service enabled  sshd.service enabled  systemd-readahead-collect.service enabled  systemd-readahead-drop.service enabled  systemd-readahead-replay.service enabled  tuned.service enabled  dm-event.socket enabled  lvm2-lvmetad.socket enabled  lvm2-lvmpolld.socket enabled  default.target enabled  multi-user.target enabled  remote-fs.target enabled  runlevel2.target enabled  runlevel3.target enabled  runlevel4.target enabled |
| **加固方法** | 与管理员确定不需要启动的服务，如telnet、ftpd等。  chkconfig设置的随系统启动服务，使用命令“chkconfig --level <init级别> <服务名> off”将所有不需要使用的服务，设置服务在各init级别不随系统启动。  systemctl设置的随系统启动服务，使用命令“systemctl disable 服务名”，禁止随系统启动。 |
| **加固结果** | 未加固 |
| **回退方法** | chkconfig --level <init级别> <服务名> on 恢复服务启动 |
| **基线符合性**  **判定依据** | 关闭brt-ccpp.service、abrt-oops.service、abrt-vmcore.service、abrt-xorg.service、abrtd.service、dbus-org.freedesktop.NetworkManager.service、NetworkManager-dispatcher.service、postfix.service、snmpd、telnet、ftpd等服务。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **SSH服务安全配置**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-04-02-01** |
| **操作目的** | 检查SSH服务安全配置，确保远程访问安全。 |
| **检查方法** | 使用命令“cat /etc/ssh/sshd\_config”查看配置文件：  Port 22222 #port用来设置sshd监听的端口，为了安全起见，建议更改默认的22端口为22222；  Protocol 2 #Protocol 2,1设置协议版本为SSH1或SSH2，SSH1存在漏洞与缺陷，选择SSH2；  ListenAddress 0.0.0.0 #ListenAddress用来设置sshd服务器绑定的IP地址，设置为指定的IP地址；  LoginGraceTime 5m #LoginGraceTime用来设定如果用户登录失败，在切断连接前服务器需要等待的时间；  MaxAuthTries 10 #允许登录尝试错误次数  PermitRootLogin no #PermitRootLogin用来设置能不能直接以超级用户ssh登录，root远程登录Linux很危险，设置为no  StrictModes yes #StrictModes用来设置ssh在接收登录请求之前是否检查用户根目录和rhosts文件的权限和所有权，建议开启来预防可能出现的低级错误  PasswordAuthentication yes #PasswordAuthentication用来设置是否开启密码验证机制，如果用密码登录系统，则设置yes  PermitEmptyPasswords no #PermitEmptyPasswords用来设置是否允许用口令为空的账号登录系统，设置no  AllowUsers <用户名1> <用户名2> <用户名3> #指定允许通过远程访问的用户，多个用户以空格隔开  AllowGroups<组名1> <组名2> <组名3> #指定允许通过远程访问的组，多个组以空格隔开。当多个用户需要通过ssh登录系统时，可将所有用户加入一个组中。 |
| **检查结果** | 是否符合：  不符合，默认配置。  现状：  # $OpenBSD: sshd\_config,v 1.100 2016/08/15 12:32:04 naddy Exp $  # This is the sshd server system-wide configuration file. See # sshd\_config(5) for more information.  # This sshd was compiled with PATH=/usr/local/bin:/usr/bin  # The strategy used for options in the default sshd\_config shipped with # OpenSSH is to specify options with their default value where # possible, but leave them commented. Uncommented options override the # default value.  # If you want to change the port on a SELinux system, you have to tell # SELinux about this change. # semanage port -a -t ssh\_port\_t -p tcp #PORTNUMBER # #Port 22 #AddressFamily any #ListenAddress 0.0.0.0 #ListenAddress ::  HostKey /etc/ssh/ssh\_host\_rsa\_key #HostKey /etc/ssh/ssh\_host\_dsa\_key HostKey /etc/ssh/ssh\_host\_ecdsa\_key HostKey /etc/ssh/ssh\_host\_ed25519\_key  # Ciphers and keying #RekeyLimit default none  # Logging #SyslogFacility AUTH SyslogFacility AUTHPRIV #LogLevel INFO  # Authentication:  #LoginGraceTime 2m #PermitRootLogin yes #StrictModes yes #MaxAuthTries 6 #MaxSessions 10  #PubkeyAuthentication yes  # The default is to check both .ssh/authorized\_keys and .ssh/authorized\_keys2 # but this is overridden so installations will only check .ssh/authorized\_keys AuthorizedKeysFile .ssh/authorized\_keys  #AuthorizedPrincipalsFile none  #AuthorizedKeysCommand none #AuthorizedKeysCommandUser nobody  # For this to work you will also need host keys in /etc/ssh/ssh\_known\_hosts #HostbasedAuthentication no # Change to yes if you don't trust ~/.ssh/known\_hosts for # HostbasedAuthentication #IgnoreUserKnownHosts no # Don't read the user's ~/.rhosts and ~/.shosts files #IgnoreRhosts yes  # To disable tunneled clear text passwords, change to no here! #PasswordAuthentication yes #PermitEmptyPasswords no PasswordAuthentication yes  # Change to no to disable s/key passwords #ChallengeResponseAuthentication yes ChallengeResponseAuthentication no  # Kerberos options #KerberosAuthentication no #KerberosOrLocalPasswd yes #KerberosTicketCleanup yes #KerberosGetAFSToken no #KerberosUseKuserok yes  # GSSAPI options GSSAPIAuthentication yes GSSAPICleanupCredentials no #GSSAPIStrictAcceptorCheck yes #GSSAPIKeyExchange no #GSSAPIEnablek5users no  # Set this to 'yes' to enable PAM authentication, account processing, # and session processing. If this is enabled, PAM authentication will # be allowed through the ChallengeResponseAuthentication and # PasswordAuthentication. Depending on your PAM configuration, # PAM authentication via ChallengeResponseAuthentication may bypass # the setting of "PermitRootLogin without-password". # If you just want the PAM account and session checks to run without # PAM authentication, then enable this but set PasswordAuthentication # and ChallengeResponseAuthentication to 'no'. # WARNING: 'UsePAM no' is not supported in Red Hat Enterprise Linux and may cause several # problems. UsePAM yes  #AllowAgentForwarding yes #AllowTcpForwarding yes #GatewayPorts no X11Forwarding yes #X11DisplayOffset 10 #X11UseLocalhost yes #PermitTTY yes #PrintMotd yes #PrintLastLog yes #TCPKeepAlive yes #UseLogin no #UsePrivilegeSeparation sandbox #PermitUserEnvironment no #Compression delayed #ClientAliveInterval 0 #ClientAliveCountMax 3 #ShowPatchLevel no #UseDNS yes #PidFile /var/run/sshd.pid #MaxStartups 10:30:100 #PermitTunnel no #ChrootDirectory none #VersionAddendum none  # no default banner path #Banner none  # Accept locale-related environment variables AcceptEnv LANG LC\_CTYPE LC\_NUMERIC LC\_TIME LC\_COLLATE LC\_MONETARY LC\_MESSAGES AcceptEnv LC\_PAPER LC\_NAME LC\_ADDRESS LC\_TELEPHONE LC\_MEASUREMENT AcceptEnv LC\_IDENTIFICATION LC\_ALL LANGUAGE AcceptEnv XMODIFIERS  # override default of no subsystems Subsystem sftp /usr/libexec/openssh/sftp-server  # Example of overriding settings on a per-user basis #Match User anoncvs # X11Forwarding no # AllowTcpForwarding no # PermitTTY no # ForceCommand cvs server |
| **加固方法** | 备份“cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.bak”;  使用命令“vim /etc/ssh/sshd\_config”编辑配置文件，确保配置为：  Port 22222  Protocol 2  ListenAddress 192.168.0.8 #根据实际修改  PermitRootLogin no  LoginGraceTime 5m  MaxAuthTries 10  StrictModes yes  PasswordAuthentication yes  PermitEmptyPasswords no  AllowUsers test1 test2 #根据实际修改  AllowGroups test #根据实际修改  2、添加普通用户，设置无需输入密码即可sudo到root，  ①添加用户：“useradd hngcadmin”。  ②设置密码：“passwd hngcadmin”  输入密码”qpalzm2021@)@!”  再次输入”qpalzm2021@)@!”  ③“sudoedit /etc/sudoers”添加一行配置  hngcadmin ALL=(ALL) NOPASSWD: ALL |
| **加固结果** | 未加固 |
| **回退方法** | cp /etc/ssh/sshd\_config.bak /etc/ssh/sshd\_config |
| **基线符合性**  **判定依据** | 只允许test用户组test1、test2用户通过密码认证方式访问192.168.0.8 22222；登录尝试错误10次后系统锁定5分钟； |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 一般通过普通用户访问sshd服务，可以通过su root提升特定用户为root权限。 |

* + - 1. **检查.rhosts和/etc/hosts.equiv文件**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-04-03-01** |
| **操作目的** | 检查.rhosts和/etc/hosts.equiv文件，防止配置错误导致非授权的访问风险。 |
| **检查方法** | 1）使用“find / -name .rhosts -print”查找.rhosts文件，若.rhosts文件中包含远程主机名，则代表允许该主机通过rlogin等方式登录本机；如果包含两个加号，代表任何主机都可以无需用户名口令登录本机  2）使用“cat /etc/hosts.equiv”查看配置文件，若包含远程主机名，则代表允许该主机远程登录本机 |
| **检查结果** | 是否符合：  符合  现状：  未发现 |
| **加固方法** | 使用命令“vim .rhosts”和“vim /etc/hosts.equiv”修改配置文件，正确进行授权 |
| **加固结果** | 未加固 |
| **回退方法** | 使用命令“vim .rhosts”和“vim /etc/hosts.equiv”将配置改回加固前 |
| **基线符合性**  **判定依据** | .rhosts和/etc/hosts.equiv文件中设定的主机可以访问，其他一律拒绝。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **配置TCP Wrapper访问控制**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-04-04-01** |
| **操作目的** | 使用TCP Wrapper对libwrap库支持的程序做访问控制 |
| **检查方法** | 使用命令“cat /etc/hosts.allow”和“cat /etc/hosts.deny”查看配置 |
| **检查结果** | 是否符合：  不适用  现状：  # # hosts.allow This file contains access rules which are used to # allow or deny connections to network services that # either use the tcp\_wrappers library or that have been # started through a tcp\_wrappers-enabled xinetd. # # See 'man 5 hosts\_options' and 'man 5 hosts\_access' # for information on rule syntax. # See 'man tcpd' for information on tcp\_wrappers # # # hosts.deny This file contains access rules which are used to # deny connections to network services that either use # the tcp\_wrappers library or that have been # started through a tcp\_wrappers-enabled xinetd. # # The rules in this file can also be set up in # /etc/hosts.allow with a 'deny' option instead. # # See 'man 5 hosts\_options' and 'man 5 hosts\_access' # for information on rule syntax. # See 'man tcpd' for information on tcp\_wrappers # |
| **加固方法** | 使用命令“vim /etc/hosts.allow”和“vim /etc/hosts.deny”修改配置文件。  vim /etc/hosts.allow打开配置文件，增加条目：  #只允许指定的IP访问sshd服务  sshd:IP地址  vim /etc/hosts.deny打开配置文件，增加条目：  #禁止所有主机访问sshd服务  Sshd:ALL:deny |
| **加固结果** | 防火墙有设置，对业务需求暂不清晰，不在主机上设置 |
| **回退方法** | 使用命令“vim /etc/hosts.allow”和“vim /etc/hosts.deny”将配置改回加固前 |
| **基线符合性**  **判定依据** | 只有指定的IP可以访问指定的服务 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **防止误使用Ctrl+Alt+Del重启系统**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-04-05-01** |
| **操作目的** | 防止误使用Ctrl+Alt+Del重启系统 |
| **检查方法** | 使用命令“cat /etc/inittab|grep ctrlaltdel”查看输入行是否被注释  #查看/etc/inittab确认Ctrl+Alt+Del相关配置文件  cat /etc/inittab  # Ctrl-Alt-Delete is handled by /usr/lib/systemd/system/ctrl-alt-del.target #相关配置文件存放位置  #查看Ctrl+Alt+Del配置文件的属性信息  ls -ld /usr/lib/systemd/system/ctrl-alt-del.target  lrwxrwxrwx. 1 root root 13 Jun 14 02:20 /usr/lib/systemd/system/ctrl-alt-del.target -> reboot.target  #删除软链接文件  rm -f /usr/lib/systemd/system/ctrl-alt-del.target或者mv /usr/lib/systemd/system/ctrl-alt-del.target /tmp  #重新加载初始化守护进程配置文件(Reload init daemon configuration)  init q |
| **检查结果** | 是否符合：  不符合  现状：  # inittab is no longer used when using systemd. # # ADDING CONFIGURATION HERE WILL HAVE NO EFFECT ON YOUR SYSTEM. # # Ctrl-Alt-Delete is handled by /usr/lib/systemd/system/ctrl-alt-del.target # # systemd uses 'targets' instead of runlevels. By default, there are two main targets: # # multi-user.target: analogous to runlevel 3 # graphical.target: analogous to runlevel 5 # # To view current default target, run: # systemctl get-default # # To set a default target, run: # systemctl set-default TARGET.target # # This file is part of systemd. # # systemd is free software; you can redistribute it and/or modify it # under the terms of the GNU Lesser General Public License as published by # the Free Software Foundation; either version 2.1 of the License, or # (at your option) any later version.  [Unit] Description=Reboot Documentation=man:systemd.special(7) DefaultDependencies=no Requires=systemd-reboot.service After=systemd-reboot.service AllowIsolate=yes JobTimeoutSec=30min JobTimeoutAction=reboot-force  [Install] Alias=ctrl-alt-del.target |
| **加固方法** | 先使用命令“vim /etc/inittab”编辑配置文件，在ctrlaltdel行开头添加注释符号“#”:  #ca::ctrlaltdel:/sbin/shutdown -t3 -r now，再使用命令“init q”应用设置 |
| **加固结果** | 未加固 |
| **回退方法** | 先使用命令“vim /etc/inittab”编辑配置文件去掉注释：ca::ctrlaltdel:/sbin/shutdown -t3 -r now，再使用命令“init q”应用设置 |
| **基线符合性**  **判定依据** | 使用Ctrl+Alt+Del命令，Linux系统不重启 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **FTP服务安全配置**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-04-06-01** |
| **操作目的** | 安全配置FTP服务，确保开放服务安全 |
| **检查方法** | vim /etc/vsftpd/vsftpd.conf打开配置文件：  anonymous\_enable=NO #不允许匿名用户  userlist\_enable=YES #禁止/etc/vsftpd/user\_list用户列表中的用户登录  vim /etc/vsftpd/user\_list打开配置文件，应该有如下用户：  root、bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、nobody、ftp |
| **检查结果** | 是否符合：  不适用  现状：  没有找到配置文件 |
| **加固方法** | 1.禁止提供匿名FTP服务，禁止匿名FTP服务  vim /etc/vsftpd/vsftpd.conf  把 anonymous\_enable=YES 修改为anonymous\_enable=NO  2. 禁止root等特定用户ftp登录  vim /etc/vsftpd/vsftpd.conf  增加“userlist\_enable=YES”  vim /etc/vsftpd/user\_list打开配置文件，增加如下用户（每个用户一行）：  root、bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、nobody、ftp  3.重新启动VSFTPD  service vsftpd restart |
| **加固结果** | 未加固 |
| **回退方法** | vim /etc/vsftpd/vsftpd.conf  vim /etc/vsftpd/user\_list  将配置还原到加固前值。 |
| **基线符合性**  **判定依据** | root、bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、nobody、ftp不能登录。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + 1. **网络参数**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-05-01-01** |
| **操作目的** | Linux中提供了sysctl命令，可调整网络参数 |
| **检查方法** | 使用命令“sysctl -A”查看当前网络参数 |
| **检查结果** | 是否符合：  不适用  现状：  abi.vsyscall32 = 1 crypto.fips\_enabled = 0 debug.exception-trace = 1 debug.kprobes-optimization = 1 debug.panic\_on\_rcu\_stall = 0 dev.hpet.max-user-freq = 64 dev.mac\_hid.mouse\_button2\_keycode = 97 dev.mac\_hid.mouse\_button3\_keycode = 100 dev.mac\_hid.mouse\_button\_emulation = 0 dev.parport.default.spintime = 500 dev.parport.default.timeslice = 200 dev.raid.speed\_limit\_max = 200000 dev.raid.speed\_limit\_min = 1000 dev.scsi.logging\_level = 0 fs.aio-max-nr = 65536 fs.aio-nr = 0 fs.binfmt\_misc.status = enabled fs.dentry-state = 67993 52320 45 0 7840 0 fs.dir-notify-enable = 1 fs.epoll.max\_user\_watches = 376688 fs.file-max = 179715 fs.file-nr = 1824 0 179715 fs.inode-nr = 60525 345 fs.inode-state = 60525 345 0 0 0 0 0 fs.inotify.max\_queued\_events = 16384 fs.inotify.max\_user\_instances = 128 fs.inotify.max\_user\_watches = 8192 fs.lease-break-time = 45 fs.leases-enable = 1 fs.may\_detach\_mounts = 0 fs.mount-max = 100000 fs.mqueue.msg\_default = 10 fs.mqueue.msg\_max = 10 fs.mqueue.msgsize\_default = 8192 fs.mqueue.msgsize\_max = 8192 fs.mqueue.queues\_max = 256 fs.negative-dentry-limit = 0 fs.nr\_open = 1048576 fs.overflowgid = 65534 fs.overflowuid = 65534 fs.pipe-max-size = 1048576 fs.pipe-user-pages-hard = 0 fs.pipe-user-pages-soft = 16384 fs.protected\_hardlinks = 1 fs.protected\_symlinks = 1 fs.quota.allocated\_dquots = 0 fs.quota.cache\_hits = 0 fs.quota.drops = 0 fs.quota.free\_dquots = 0 fs.quota.lookups = 0 fs.quota.reads = 0 fs.quota.syncs = 0 fs.quota.warnings = 1 fs.quota.writes = 0 fs.suid\_dumpable = 0 fs.xfs.age\_buffer\_centisecs = 1500 fs.xfs.error\_level = 3 fs.xfs.filestream\_centisecs = 3000 fs.xfs.inherit\_noatime = 1 fs.xfs.inherit\_nodefrag = 1 fs.xfs.inherit\_nodump = 1 fs.xfs.inherit\_nosymlinks = 0 fs.xfs.inherit\_sync = 1 fs.xfs.irix\_sgid\_inherit = 0 fs.xfs.irix\_symlink\_mode = 0 fs.xfs.panic\_mask = 0 fs.xfs.rotorstep = 1 fs.xfs.speculative\_prealloc\_lifetime = 300 fs.xfs.stats\_clear = 0 fs.xfs.xfsbufd\_centisecs = 100 fs.xfs.xfssyncd\_centisecs = 3000 kernel.acct = 4 2 30 kernel.acpi\_video\_flags = 0 kernel.auto\_msgmni = 0 kernel.bootloader\_type = 114 kernel.bootloader\_version = 2 kernel.cad\_pid = 1 kernel.cap\_last\_cap = 36 kernel.compat-log = 1 kernel.core\_pattern = core kernel.core\_pipe\_limit = 0 kernel.core\_uses\_pid = 1 kernel.ctrl-alt-del = 0 kernel.dmesg\_restrict = 0 kernel.domainname = (none) kernel.ftrace\_dump\_on\_oops = 0 kernel.ftrace\_enabled = 1 kernel.hardlockup\_all\_cpu\_backtrace = 0 kernel.hardlockup\_panic = 1 kernel.hostname = localhost.localdomain kernel.hotplug =  kernel.hung\_task\_check\_count = 4194304 kernel.hung\_task\_panic = 0 kernel.hung\_task\_timeout\_secs = 120 kernel.hung\_task\_warnings = 10 kernel.io\_delay\_type = 0 kernel.kexec\_load\_disabled = 0 kernel.keys.gc\_delay = 300 kernel.keys.maxbytes = 20000 kernel.keys.maxkeys = 200 kernel.keys.persistent\_keyring\_expiry = 259200 kernel.keys.root\_maxbytes = 25000000 kernel.keys.root\_maxkeys = 1000000 kernel.kptr\_restrict = 1 kernel.max\_lock\_depth = 1024 kernel.modprobe = /sbin/modprobe kernel.modules\_disabled = 0 kernel.msg\_next\_id = -1 kernel.msgmax = 8192 kernel.msgmnb = 16384 kernel.msgmni = 32000 kernel.ngroups\_max = 65536 kernel.nmi\_watchdog = 1 kernel.ns\_last\_pid = 120498 kernel.numa\_balancing = 0 kernel.numa\_balancing\_scan\_delay\_ms = 1000 kernel.numa\_balancing\_scan\_period\_max\_ms = 60000 kernel.numa\_balancing\_scan\_period\_min\_ms = 1000 kernel.numa\_balancing\_scan\_size\_mb = 256 kernel.numa\_balancing\_settle\_count = 4 kernel.osrelease = 3.10.0-1160.42.2.el7.x86\_64 kernel.ostype = Linux kernel.overflowgid = 65534 kernel.overflowuid = 65534 kernel.panic = 0 kernel.panic\_on\_io\_nmi = 0 kernel.panic\_on\_oops = 1 kernel.panic\_on\_stackoverflow = 0 kernel.panic\_on\_unrecovered\_nmi = 0 kernel.panic\_on\_warn = 0 kernel.perf\_cpu\_time\_max\_percent = 25 kernel.perf\_event\_max\_sample\_rate = 100000 kernel.perf\_event\_mlock\_kb = 516 kernel.perf\_event\_paranoid = 2 kernel.pid\_max = 131072 kernel.poweroff\_cmd = /sbin/poweroff kernel.print-fatal-signals = 0 kernel.printk = 4 4 1 7 kernel.printk\_delay = 0 kernel.printk\_ratelimit = 5 kernel.printk\_ratelimit\_burst = 10 kernel.pty.max = 4096 kernel.pty.nr = 2 kernel.pty.reserve = 1024 kernel.random.boot\_id = f3fd7912-887e-456c-8073-f24b9b625c36 kernel.random.entropy\_avail = 3278 kernel.random.poolsize = 4096 kernel.random.read\_wakeup\_threshold = 64 kernel.random.urandom\_min\_reseed\_secs = 60 kernel.random.uuid = eb27e1db-1b49-461a-8b14-e497703103e6 kernel.random.write\_wakeup\_threshold = 896 kernel.randomize\_va\_space = 2 kernel.real-root-dev = 0 kernel.sched\_autogroup\_enabled = 0 kernel.sched\_cfs\_bandwidth\_slice\_us = 5000 kernel.sched\_child\_runs\_first = 0 kernel.sched\_domain.cpu0.domain0.busy\_factor = 32 kernel.sched\_domain.cpu0.domain0.busy\_idx = 2 kernel.sched\_domain.cpu0.domain0.cache\_nice\_tries = 1 kernel.sched\_domain.cpu0.domain0.flags = 4143 kernel.sched\_domain.cpu0.domain0.forkexec\_idx = 0 kernel.sched\_domain.cpu0.domain0.idle\_idx = 1 kernel.sched\_domain.cpu0.domain0.imbalance\_pct = 125 kernel.sched\_domain.cpu0.domain0.max\_interval = 4 kernel.sched\_domain.cpu0.domain0.max\_newidle\_lb\_cost = 8823 kernel.sched\_domain.cpu0.domain0.min\_interval = 2 kernel.sched\_domain.cpu0.domain0.name = DIE kernel.sched\_domain.cpu0.domain0.newidle\_idx = 0 kernel.sched\_domain.cpu0.domain0.wake\_idx = 0 kernel.sched\_domain.cpu1.domain0.busy\_factor = 32 kernel.sched\_domain.cpu1.domain0.busy\_idx = 2 kernel.sched\_domain.cpu1.domain0.cache\_nice\_tries = 1 kernel.sched\_domain.cpu1.domain0.flags = 4143 kernel.sched\_domain.cpu1.domain0.forkexec\_idx = 0 kernel.sched\_domain.cpu1.domain0.idle\_idx = 1 kernel.sched\_domain.cpu1.domain0.imbalance\_pct = 125 kernel.sched\_domain.cpu1.domain0.max\_interval = 4 kernel.sched\_domain.cpu1.domain0.max\_newidle\_lb\_cost = 12121 kernel.sched\_domain.cpu1.domain0.min\_interval = 2 kernel.sched\_domain.cpu1.domain0.name = DIE kernel.sched\_domain.cpu1.domain0.newidle\_idx = 0 kernel.sched\_domain.cpu1.domain0.wake\_idx = 0 kernel.sched\_latency\_ns = 12000000 kernel.sched\_migration\_cost\_ns = 500000 kernel.sched\_min\_granularity\_ns = 10000000 kernel.sched\_nr\_migrate = 32 kernel.sched\_rr\_timeslice\_ms = 100 kernel.sched\_rt\_period\_us = 1000000 kernel.sched\_rt\_runtime\_us = 950000 kernel.sched\_schedstats = 0 kernel.sched\_shares\_window\_ns = 10000000 kernel.sched\_time\_avg\_ms = 1000 kernel.sched\_tunable\_scaling = 1 kernel.sched\_wakeup\_granularity\_ns = 15000000 kernel.seccomp.actions\_avail = kill trap errno trace allow kernel.seccomp.actions\_logged = kill trap errno trace kernel.sem = 250 32000 32 128 kernel.sem\_next\_id = -1 kernel.shm\_next\_id = -1 kernel.shm\_rmid\_forced = 0 kernel.shmall = 18446744073692774399 kernel.shmmax = 18446744073692774399 kernel.shmmni = 4096 kernel.softlockup\_all\_cpu\_backtrace = 0 kernel.softlockup\_panic = 0 kernel.stack\_tracer\_enabled = 0 kernel.sysctl\_writes\_strict = 1 kernel.sysrq = 16 kernel.tainted = 0 kernel.threads-max = 14369 kernel.timer\_migration = 1 kernel.traceoff\_on\_warning = 0 kernel.unknown\_nmi\_panic = 0 kernel.usermodehelper.bset = 4294967295 31 kernel.usermodehelper.inheritable = 4294967295 31 kernel.version = #1 SMP Tue Sep 7 14:49:57 UTC 2021 kernel.watchdog = 1 kernel.watchdog\_cpumask = 0-127 kernel.watchdog\_thresh = 10 kernel.yama.ptrace\_scope = 0 net.core.bpf\_jit\_enable = 1 net.core.bpf\_jit\_harden = 1 net.core.bpf\_jit\_kallsyms = 0 net.core.busy\_poll = 0 net.core.busy\_read = 0 net.core.default\_qdisc = pfifo\_fast net.core.dev\_weight = 64 net.core.dev\_weight\_rx\_bias = 1 net.core.dev\_weight\_tx\_bias = 1 net.core.message\_burst = 10 net.core.message\_cost = 5 net.core.netdev\_budget = 300 net.core.netdev\_max\_backlog = 1000 net.core.netdev\_rss\_key = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 net.core.netdev\_tstamp\_prequeue = 1 net.core.optmem\_max = 20480 net.core.rmem\_default = 212992 net.core.rmem\_max = 212992 net.core.rps\_sock\_flow\_entries = 0 net.core.somaxconn = 128 net.core.warnings = 1 net.core.wmem\_default = 212992 net.core.wmem\_max = 212992 net.core.xfrm\_acq\_expires = 30 net.core.xfrm\_aevent\_etime = 10 net.core.xfrm\_aevent\_rseqth = 2 net.core.xfrm\_larval\_drop = 1 net.ipv4.cipso\_cache\_bucket\_size = 10 net.ipv4.cipso\_cache\_enable = 1 net.ipv4.cipso\_rbm\_optfmt = 0 net.ipv4.cipso\_rbm\_strictvalid = 1 net.ipv4.conf.all.accept\_local = 0 net.ipv4.conf.all.accept\_redirects = 1 net.ipv4.conf.all.accept\_source\_route = 0 net.ipv4.conf.all.arp\_accept = 0 net.ipv4.conf.all.arp\_announce = 0 net.ipv4.conf.all.arp\_filter = 0 net.ipv4.conf.all.arp\_ignore = 0 net.ipv4.conf.all.arp\_notify = 0 net.ipv4.conf.all.bootp\_relay = 0 net.ipv4.conf.all.disable\_policy = 0 net.ipv4.conf.all.disable\_xfrm = 0 net.ipv4.conf.all.force\_igmp\_version = 0 net.ipv4.conf.all.forwarding = 0 net.ipv4.conf.all.igmpv2\_unsolicited\_report\_interval = 10000 net.ipv4.conf.all.igmpv3\_unsolicited\_report\_interval = 1000 net.ipv4.conf.all.log\_martians = 0 net.ipv4.conf.all.mc\_forwarding = 0 net.ipv4.conf.all.medium\_id = 0 net.ipv4.conf.all.promote\_secondaries = 1 net.ipv4.conf.all.proxy\_arp = 0 net.ipv4.conf.all.proxy\_arp\_pvlan = 0 net.ipv4.conf.all.route\_localnet = 0 net.ipv4.conf.all.rp\_filter = 1 net.ipv4.conf.all.secure\_redirects = 1 net.ipv4.conf.all.send\_redirects = 1 net.ipv4.conf.all.shared\_media = 1 net.ipv4.conf.all.src\_valid\_mark = 0 net.ipv4.conf.all.tag = 0 net.ipv4.conf.default.accept\_local = 0 net.ipv4.conf.default.accept\_redirects = 1 net.ipv4.conf.default.accept\_source\_route = 0 net.ipv4.conf.default.arp\_accept = 0 net.ipv4.conf.default.arp\_announce = 0 net.ipv4.conf.default.arp\_filter = 0 net.ipv4.conf.default.arp\_ignore = 0 net.ipv4.conf.default.arp\_notify = 0 net.ipv4.conf.default.bootp\_relay = 0 net.ipv4.conf.default.disable\_policy = 0 net.ipv4.conf.default.disable\_xfrm = 0 net.ipv4.conf.default.force\_igmp\_version = 0 net.ipv4.conf.default.forwarding = 0 net.ipv4.conf.default.igmpv2\_unsolicited\_report\_interval = 10000 net.ipv4.conf.default.igmpv3\_unsolicited\_report\_interval = 1000 net.ipv4.conf.default.log\_martians = 0 net.ipv4.conf.default.mc\_forwarding = 0 net.ipv4.conf.default.medium\_id = 0 net.ipv4.conf.default.promote\_secondaries = 1 net.ipv4.conf.default.proxy\_arp = 0 net.ipv4.conf.default.proxy\_arp\_pvlan = 0 net.ipv4.conf.default.route\_localnet = 0 net.ipv4.conf.default.rp\_filter = 1 net.ipv4.conf.default.secure\_redirects = 1 net.ipv4.conf.default.send\_redirects = 1 net.ipv4.conf.default.shared\_media = 1 net.ipv4.conf.default.src\_valid\_mark = 0 net.ipv4.conf.default.tag = 0 net.ipv4.conf.ens33.accept\_local = 0 net.ipv4.conf.ens33.accept\_redirects = 1 net.ipv4.conf.ens33.accept\_source\_route = 0 net.ipv4.conf.ens33.arp\_accept = 0 net.ipv4.conf.ens33.arp\_announce = 0 net.ipv4.conf.ens33.arp\_filter = 0 net.ipv4.conf.ens33.arp\_ignore = 0 net.ipv4.conf.ens33.arp\_notify = 0 net.ipv4.conf.ens33.bootp\_relay = 0 net.ipv4.conf.ens33.disable\_policy = 0 net.ipv4.conf.ens33.disable\_xfrm = 0 net.ipv4.conf.ens33.force\_igmp\_version = 0 net.ipv4.conf.ens33.forwarding = 0 net.ipv4.conf.ens33.igmpv2\_unsolicited\_report\_interval = 10000 net.ipv4.conf.ens33.igmpv3\_unsolicited\_report\_interval = 1000 net.ipv4.conf.ens33.log\_martians = 0 net.ipv4.conf.ens33.mc\_forwarding = 0 net.ipv4.conf.ens33.medium\_id = 0 net.ipv4.conf.ens33.promote\_secondaries = 1 net.ipv4.conf.ens33.proxy\_arp = 0 net.ipv4.conf.ens33.proxy\_arp\_pvlan = 0 net.ipv4.conf.ens33.route\_localnet = 0 net.ipv4.conf.ens33.rp\_filter = 1 net.ipv4.conf.ens33.secure\_redirects = 1 net.ipv4.conf.ens33.send\_redirects = 1 net.ipv4.conf.ens33.shared\_media = 1 net.ipv4.conf.ens33.src\_valid\_mark = 0 net.ipv4.conf.ens33.tag = 0 net.ipv4.conf.lo.accept\_local = 0 net.ipv4.conf.lo.accept\_redirects = 1 net.ipv4.conf.lo.accept\_source\_route = 1 net.ipv4.conf.lo.arp\_accept = 0 net.ipv4.conf.lo.arp\_announce = 0 net.ipv4.conf.lo.arp\_filter = 0 net.ipv4.conf.lo.arp\_ignore = 0 net.ipv4.conf.lo.arp\_notify = 0 net.ipv4.conf.lo.bootp\_relay = 0 net.ipv4.conf.lo.disable\_policy = 1 net.ipv4.conf.lo.disable\_xfrm = 1 net.ipv4.conf.lo.force\_igmp\_version = 0 net.ipv4.conf.lo.forwarding = 0 net.ipv4.conf.lo.igmpv2\_unsolicited\_report\_interval = 10000 net.ipv4.conf.lo.igmpv3\_unsolicited\_report\_interval = 1000 net.ipv4.conf.lo.log\_martians = 0 net.ipv4.conf.lo.mc\_forwarding = 0 net.ipv4.conf.lo.medium\_id = 0 net.ipv4.conf.lo.promote\_secondaries = 0 net.ipv4.conf.lo.proxy\_arp = 0 net.ipv4.conf.lo.proxy\_arp\_pvlan = 0 net.ipv4.conf.lo.route\_localnet = 0 net.ipv4.conf.lo.rp\_filter = 0 net.ipv4.conf.lo.secure\_redirects = 1 net.ipv4.conf.lo.send\_redirects = 1 net.ipv4.conf.lo.shared\_media = 1 net.ipv4.conf.lo.src\_valid\_mark = 0 net.ipv4.conf.lo.tag = 0 net.ipv4.fib\_multipath\_hash\_policy = 0 net.ipv4.fwmark\_reflect = 0 net.ipv4.icmp\_echo\_ignore\_all = 0 net.ipv4.icmp\_echo\_ignore\_broadcasts = 1 net.ipv4.icmp\_errors\_use\_inbound\_ifaddr = 0 net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1 net.ipv4.icmp\_msgs\_burst = 50 net.ipv4.icmp\_msgs\_per\_sec = 1000 net.ipv4.icmp\_ratelimit = 1000 net.ipv4.icmp\_ratemask = 6168 net.ipv4.igmp\_max\_memberships = 20 net.ipv4.igmp\_max\_msf = 10 net.ipv4.igmp\_qrv = 2 net.ipv4.inet\_peer\_maxttl = 600 net.ipv4.inet\_peer\_minttl = 120 net.ipv4.inet\_peer\_threshold = 65664 net.ipv4.ip\_default\_ttl = 64 net.ipv4.ip\_dynaddr = 0 net.ipv4.ip\_early\_demux = 1 net.ipv4.ip\_forward = 0 net.ipv4.ip\_forward\_use\_pmtu = 0 net.ipv4.ip\_local\_port\_range = 32768 60999 net.ipv4.ip\_local\_reserved\_ports =  net.ipv4.ip\_no\_pmtu\_disc = 0 net.ipv4.ip\_nonlocal\_bind = 0 net.ipv4.ipfrag\_high\_thresh = 4194304 net.ipv4.ipfrag\_low\_thresh = 3145728 net.ipv4.ipfrag\_max\_dist = 64 net.ipv4.ipfrag\_secret\_interval = 600 net.ipv4.ipfrag\_time = 30 net.ipv4.neigh.default.anycast\_delay = 100 net.ipv4.neigh.default.app\_solicit = 0 net.ipv4.neigh.default.base\_reachable\_time\_ms = 30000 net.ipv4.neigh.default.delay\_first\_probe\_time = 5 net.ipv4.neigh.default.gc\_interval = 30 net.ipv4.neigh.default.gc\_stale\_time = 60 net.ipv4.neigh.default.gc\_thresh1 = 128 net.ipv4.neigh.default.gc\_thresh2 = 512 net.ipv4.neigh.default.gc\_thresh3 = 1024 net.ipv4.neigh.default.locktime = 100 net.ipv4.neigh.default.mcast\_solicit = 3 net.ipv4.neigh.default.proxy\_delay = 80 net.ipv4.neigh.default.proxy\_qlen = 64 net.ipv4.neigh.default.retrans\_time\_ms = 1000 net.ipv4.neigh.default.ucast\_solicit = 3 net.ipv4.neigh.default.unres\_qlen = 31 net.ipv4.neigh.default.unres\_qlen\_bytes = 65536 net.ipv4.neigh.ens33.anycast\_delay = 100 net.ipv4.neigh.ens33.app\_solicit = 0 net.ipv4.neigh.ens33.base\_reachable\_time\_ms = 30000 net.ipv4.neigh.ens33.delay\_first\_probe\_time = 5 net.ipv4.neigh.ens33.gc\_stale\_time = 60 net.ipv4.neigh.ens33.locktime = 100 net.ipv4.neigh.ens33.mcast\_solicit = 3 net.ipv4.neigh.ens33.proxy\_delay = 80 net.ipv4.neigh.ens33.proxy\_qlen = 64 net.ipv4.neigh.ens33.retrans\_time\_ms = 1000 net.ipv4.neigh.ens33.ucast\_solicit = 3 net.ipv4.neigh.ens33.unres\_qlen = 31 net.ipv4.neigh.ens33.unres\_qlen\_bytes = 65536 net.ipv4.neigh.lo.anycast\_delay = 100 net.ipv4.neigh.lo.app\_solicit = 0 net.ipv4.neigh.lo.base\_reachable\_time\_ms = 30000 net.ipv4.neigh.lo.delay\_first\_probe\_time = 5 net.ipv4.neigh.lo.gc\_stale\_time = 60 net.ipv4.neigh.lo.locktime = 100 net.ipv4.neigh.lo.mcast\_solicit = 3 net.ipv4.neigh.lo.proxy\_delay = 80 net.ipv4.neigh.lo.proxy\_qlen = 64 net.ipv4.neigh.lo.retrans\_time\_ms = 1000 net.ipv4.neigh.lo.ucast\_solicit = 3 net.ipv4.neigh.lo.unres\_qlen = 31 net.ipv4.neigh.lo.unres\_qlen\_bytes = 65536 net.ipv4.ping\_group\_range = 1 0 net.ipv4.route.error\_burst = 5000 net.ipv4.route.error\_cost = 1000 net.ipv4.route.gc\_elasticity = 8 net.ipv4.route.gc\_interval = 60 net.ipv4.route.gc\_min\_interval = 0 net.ipv4.route.gc\_min\_interval\_ms = 500 net.ipv4.route.gc\_thresh = -1 net.ipv4.route.gc\_timeout = 300 net.ipv4.route.max\_size = 2147483647 net.ipv4.route.min\_adv\_mss = 256 net.ipv4.route.min\_pmtu = 552 net.ipv4.route.mtu\_expires = 600 net.ipv4.route.redirect\_load = 20 net.ipv4.route.redirect\_number = 9 net.ipv4.route.redirect\_silence = 20480 net.ipv4.tcp\_abort\_on\_overflow = 0 net.ipv4.tcp\_adv\_win\_scale = 1 net.ipv4.tcp\_allowed\_congestion\_control = cubic reno net.ipv4.tcp\_app\_win = 31 net.ipv4.tcp\_autocorking = 1 net.ipv4.tcp\_available\_congestion\_control = cubic reno net.ipv4.tcp\_base\_mss = 512 net.ipv4.tcp\_challenge\_ack\_limit = 1000 net.ipv4.tcp\_congestion\_control = cubic net.ipv4.tcp\_dsack = 1 net.ipv4.tcp\_early\_retrans = 3 net.ipv4.tcp\_ecn = 2 net.ipv4.tcp\_fack = 1 net.ipv4.tcp\_fastopen = 0 net.ipv4.tcp\_fastopen\_key = 00000000-00000000-00000000-00000000 net.ipv4.tcp\_fin\_timeout = 60 net.ipv4.tcp\_frto = 2 net.ipv4.tcp\_invalid\_ratelimit = 500 net.ipv4.tcp\_keepalive\_intvl = 75 net.ipv4.tcp\_keepalive\_probes = 9 net.ipv4.tcp\_keepalive\_time = 7200 net.ipv4.tcp\_limit\_output\_bytes = 262144 net.ipv4.tcp\_low\_latency = 0 net.ipv4.tcp\_max\_orphans = 8192 net.ipv4.tcp\_max\_ssthresh = 0 net.ipv4.tcp\_max\_syn\_backlog = 128 net.ipv4.tcp\_max\_tw\_buckets = 8192 net.ipv4.tcp\_mem = 42012 56017 84024 net.ipv4.tcp\_min\_snd\_mss = 48 net.ipv4.tcp\_min\_tso\_segs = 2 net.ipv4.tcp\_moderate\_rcvbuf = 1 net.ipv4.tcp\_mtu\_probing = 0 net.ipv4.tcp\_no\_metrics\_save = 0 net.ipv4.tcp\_notsent\_lowat = -1 net.ipv4.tcp\_orphan\_retries = 0 net.ipv4.tcp\_reordering = 3 net.ipv4.tcp\_retrans\_collapse = 1 net.ipv4.tcp\_retries1 = 3 net.ipv4.tcp\_retries2 = 15 net.ipv4.tcp\_rfc1337 = 0 net.ipv4.tcp\_rmem = 4096 87380 6291456 net.ipv4.tcp\_sack = 1 net.ipv4.tcp\_slow\_start\_after\_idle = 1 net.ipv4.tcp\_stdurg = 0 net.ipv4.tcp\_syn\_retries = 6 net.ipv4.tcp\_synack\_retries = 5 net.ipv4.tcp\_syncookies = 1 net.ipv4.tcp\_thin\_dupack = 0 net.ipv4.tcp\_thin\_linear\_timeouts = 0 net.ipv4.tcp\_timestamps = 1 net.ipv4.tcp\_tso\_win\_divisor = 3 net.ipv4.tcp\_tw\_recycle = 0 net.ipv4.tcp\_tw\_reuse = 0 net.ipv4.tcp\_window\_scaling = 1 net.ipv4.tcp\_wmem = 4096 16384 4194304 net.ipv4.tcp\_workaround\_signed\_windows = 0 net.ipv4.udp\_mem = 43107 57479 86214 net.ipv4.udp\_rmem\_min = 4096 net.ipv4.udp\_wmem\_min = 4096 net.ipv4.xfrm4\_gc\_thresh = 32768 net.ipv6.anycast\_src\_echo\_reply = 0 net.ipv6.bindv6only = 0 net.ipv6.conf.all.accept\_dad = 0 net.ipv6.conf.all.accept\_ra = 1 net.ipv6.conf.all.accept\_ra\_defrtr = 1 net.ipv6.conf.all.accept\_ra\_pinfo = 1 net.ipv6.conf.all.accept\_ra\_rt\_info\_max\_plen = 0 net.ipv6.conf.all.accept\_ra\_rtr\_pref = 1 net.ipv6.conf.all.accept\_redirects = 1 net.ipv6.conf.all.accept\_source\_route = 0 net.ipv6.conf.all.autoconf = 1 net.ipv6.conf.all.dad\_transmits = 1 net.ipv6.conf.all.disable\_ipv6 = 0 net.ipv6.conf.all.enhanced\_dad = 1 net.ipv6.conf.all.force\_mld\_version = 0 net.ipv6.conf.all.force\_tllao = 0 net.ipv6.conf.all.forwarding = 0 net.ipv6.conf.all.hop\_limit = 64 net.ipv6.conf.all.keep\_addr\_on\_down = 0 net.ipv6.conf.all.max\_addresses = 16 net.ipv6.conf.all.max\_desync\_factor = 600 net.ipv6.conf.all.mc\_forwarding = 0 net.ipv6.conf.all.mldv1\_unsolicited\_report\_interval = 10000 net.ipv6.conf.all.mldv2\_unsolicited\_report\_interval = 1000 net.ipv6.conf.all.mtu = 1280 net.ipv6.conf.all.ndisc\_notify = 0 net.ipv6.conf.all.optimistic\_dad = 0 net.ipv6.conf.all.proxy\_ndp = 0 net.ipv6.conf.all.regen\_max\_retry = 3 net.ipv6.conf.all.router\_probe\_interval = 60 net.ipv6.conf.all.router\_solicitation\_delay = 1 net.ipv6.conf.all.router\_solicitation\_interval = 4 net.ipv6.conf.all.router\_solicitations = 3 net.ipv6.conf.all.temp\_prefered\_lft = 86400 net.ipv6.conf.all.temp\_valid\_lft = 604800 net.ipv6.conf.all.use\_optimistic = 0 net.ipv6.conf.all.use\_tempaddr = 0 net.ipv6.conf.default.accept\_dad = 1 net.ipv6.conf.default.accept\_ra = 1 net.ipv6.conf.default.accept\_ra\_defrtr = 1 net.ipv6.conf.default.accept\_ra\_pinfo = 1 net.ipv6.conf.default.accept\_ra\_rt\_info\_max\_plen = 0 net.ipv6.conf.default.accept\_ra\_rtr\_pref = 1 net.ipv6.conf.default.accept\_redirects = 1 net.ipv6.conf.default.accept\_source\_route = 0 net.ipv6.conf.default.autoconf = 1 net.ipv6.conf.default.dad\_transmits = 1 net.ipv6.conf.default.disable\_ipv6 = 0 net.ipv6.conf.default.enhanced\_dad = 1 net.ipv6.conf.default.force\_mld\_version = 0 net.ipv6.conf.default.force\_tllao = 0 net.ipv6.conf.default.forwarding = 0 net.ipv6.conf.default.hop\_limit = 64 net.ipv6.conf.default.keep\_addr\_on\_down = 0 net.ipv6.conf.default.max\_addresses = 16 net.ipv6.conf.default.max\_desync\_factor = 600 net.ipv6.conf.default.mc\_forwarding = 0 net.ipv6.conf.default.mldv1\_unsolicited\_report\_interval = 10000 net.ipv6.conf.default.mldv2\_unsolicited\_report\_interval = 1000 net.ipv6.conf.default.mtu = 1280 net.ipv6.conf.default.ndisc\_notify = 0 net.ipv6.conf.default.optimistic\_dad = 0 net.ipv6.conf.default.proxy\_ndp = 0 net.ipv6.conf.default.regen\_max\_retry = 3 net.ipv6.conf.default.router\_probe\_interval = 60 net.ipv6.conf.default.router\_solicitation\_delay = 1 net.ipv6.conf.default.router\_solicitation\_interval = 4 net.ipv6.conf.default.router\_solicitations = 3 net.ipv6.conf.default.temp\_prefered\_lft = 86400 net.ipv6.conf.default.temp\_valid\_lft = 604800 net.ipv6.conf.default.use\_optimistic = 0 net.ipv6.conf.default.use\_tempaddr = 0 net.ipv6.conf.ens33.accept\_dad = 1 net.ipv6.conf.ens33.accept\_ra = 1 net.ipv6.conf.ens33.accept\_ra\_defrtr = 0 net.ipv6.conf.ens33.accept\_ra\_pinfo = 0 net.ipv6.conf.ens33.accept\_ra\_rt\_info\_max\_plen = 0 net.ipv6.conf.ens33.accept\_ra\_rtr\_pref = 0 net.ipv6.conf.ens33.accept\_redirects = 1 net.ipv6.conf.ens33.accept\_source\_route = 0 net.ipv6.conf.ens33.autoconf = 1 net.ipv6.conf.ens33.dad\_transmits = 1 net.ipv6.conf.ens33.disable\_ipv6 = 0 net.ipv6.conf.ens33.enhanced\_dad = 1 net.ipv6.conf.ens33.force\_mld\_version = 0 net.ipv6.conf.ens33.force\_tllao = 0 net.ipv6.conf.ens33.forwarding = 0 net.ipv6.conf.ens33.hop\_limit = 64 net.ipv6.conf.ens33.keep\_addr\_on\_down = 0 net.ipv6.conf.ens33.max\_addresses = 16 net.ipv6.conf.ens33.max\_desync\_factor = 600 net.ipv6.conf.ens33.mc\_forwarding = 0 net.ipv6.conf.ens33.mldv1\_unsolicited\_report\_interval = 10000 net.ipv6.conf.ens33.mldv2\_unsolicited\_report\_interval = 1000 net.ipv6.conf.ens33.mtu = 1500 net.ipv6.conf.ens33.ndisc\_notify = 0 net.ipv6.conf.ens33.optimistic\_dad = 0 net.ipv6.conf.ens33.proxy\_ndp = 0 net.ipv6.conf.ens33.regen\_max\_retry = 3 net.ipv6.conf.ens33.router\_probe\_interval = 60 net.ipv6.conf.ens33.router\_solicitation\_delay = 1 net.ipv6.conf.ens33.router\_solicitation\_interval = 4 net.ipv6.conf.ens33.router\_solicitations = 3 net.ipv6.conf.ens33.temp\_prefered\_lft = 86400 net.ipv6.conf.ens33.temp\_valid\_lft = 604800 net.ipv6.conf.ens33.use\_optimistic = 0 net.ipv6.conf.ens33.use\_tempaddr = 0 net.ipv6.conf.lo.accept\_dad = -1 net.ipv6.conf.lo.accept\_ra = 1 net.ipv6.conf.lo.accept\_ra\_defrtr = 1 net.ipv6.conf.lo.accept\_ra\_pinfo = 1 net.ipv6.conf.lo.accept\_ra\_rt\_info\_max\_plen = 0 net.ipv6.conf.lo.accept\_ra\_rtr\_pref = 1 net.ipv6.conf.lo.accept\_redirects = 1 net.ipv6.conf.lo.accept\_source\_route = 0 net.ipv6.conf.lo.autoconf = 1 net.ipv6.conf.lo.dad\_transmits = 1 net.ipv6.conf.lo.disable\_ipv6 = 0 net.ipv6.conf.lo.enhanced\_dad = 1 net.ipv6.conf.lo.force\_mld\_version = 0 net.ipv6.conf.lo.force\_tllao = 0 net.ipv6.conf.lo.forwarding = 0 net.ipv6.conf.lo.hop\_limit = 64 net.ipv6.conf.lo.keep\_addr\_on\_down = 0 net.ipv6.conf.lo.max\_addresses = 16 net.ipv6.conf.lo.max\_desync\_factor = 600 net.ipv6.conf.lo.mc\_forwarding = 0 net.ipv6.conf.lo.mldv1\_unsolicited\_report\_interval = 10000 net.ipv6.conf.lo.mldv2\_unsolicited\_report\_interval = 1000 net.ipv6.conf.lo.mtu = 65536 net.ipv6.conf.lo.ndisc\_notify = 0 net.ipv6.conf.lo.optimistic\_dad = 0 net.ipv6.conf.lo.proxy\_ndp = 0 net.ipv6.conf.lo.regen\_max\_retry = 3 net.ipv6.conf.lo.router\_probe\_interval = 60 net.ipv6.conf.lo.router\_solicitation\_delay = 1 net.ipv6.conf.lo.router\_solicitation\_interval = 4 net.ipv6.conf.lo.router\_solicitations = 3 net.ipv6.conf.lo.temp\_prefered\_lft = 86400 net.ipv6.conf.lo.temp\_valid\_lft = 604800 net.ipv6.conf.lo.use\_optimistic = 0 net.ipv6.conf.lo.use\_tempaddr = -1 net.ipv6.fwmark\_reflect = 0 net.ipv6.icmp.ratelimit = 1000 net.ipv6.idgen\_delay = 1 net.ipv6.idgen\_retries = 3 net.ipv6.ip6frag\_high\_thresh = 4194304 net.ipv6.ip6frag\_low\_thresh = 3145728 net.ipv6.ip6frag\_secret\_interval = 600 net.ipv6.ip6frag\_time = 60 net.ipv6.ip\_nonlocal\_bind = 0 net.ipv6.mld\_max\_msf = 64 net.ipv6.mld\_qrv = 2 net.ipv6.neigh.default.anycast\_delay = 100 net.ipv6.neigh.default.app\_solicit = 0 net.ipv6.neigh.default.base\_reachable\_time\_ms = 30000 net.ipv6.neigh.default.delay\_first\_probe\_time = 5 net.ipv6.neigh.default.gc\_interval = 30 net.ipv6.neigh.default.gc\_stale\_time = 60 net.ipv6.neigh.default.gc\_thresh1 = 128 net.ipv6.neigh.default.gc\_thresh2 = 512 net.ipv6.neigh.default.gc\_thresh3 = 1024 net.ipv6.neigh.default.locktime = 0 net.ipv6.neigh.default.mcast\_solicit = 3 net.ipv6.neigh.default.proxy\_delay = 80 net.ipv6.neigh.default.proxy\_qlen = 64 net.ipv6.neigh.default.retrans\_time\_ms = 1000 net.ipv6.neigh.default.ucast\_solicit = 3 net.ipv6.neigh.default.unres\_qlen = 31 net.ipv6.neigh.default.unres\_qlen\_bytes = 65536 net.ipv6.neigh.ens33.anycast\_delay = 100 net.ipv6.neigh.ens33.app\_solicit = 0 net.ipv6.neigh.ens33.base\_reachable\_time\_ms = 30000 net.ipv6.neigh.ens33.delay\_first\_probe\_time = 5 net.ipv6.neigh.ens33.gc\_stale\_time = 60 net.ipv6.neigh.ens33.locktime = 0 net.ipv6.neigh.ens33.mcast\_solicit = 3 net.ipv6.neigh.ens33.proxy\_delay = 80 net.ipv6.neigh.ens33.proxy\_qlen = 64 net.ipv6.neigh.ens33.retrans\_time\_ms = 1000 net.ipv6.neigh.ens33.ucast\_solicit = 3 net.ipv6.neigh.ens33.unres\_qlen = 31 net.ipv6.neigh.ens33.unres\_qlen\_bytes = 65536 net.ipv6.neigh.lo.anycast\_delay = 100 net.ipv6.neigh.lo.app\_solicit = 0 net.ipv6.neigh.lo.base\_reachable\_time\_ms = 30000 net.ipv6.neigh.lo.delay\_first\_probe\_time = 5 net.ipv6.neigh.lo.gc\_stale\_time = 60 net.ipv6.neigh.lo.locktime = 0 net.ipv6.neigh.lo.mcast\_solicit = 3 net.ipv6.neigh.lo.proxy\_delay = 80 net.ipv6.neigh.lo.proxy\_qlen = 64 net.ipv6.neigh.lo.retrans\_time\_ms = 1000 net.ipv6.neigh.lo.ucast\_solicit = 3 net.ipv6.neigh.lo.unres\_qlen = 31 net.ipv6.neigh.lo.unres\_qlen\_bytes = 65536 net.ipv6.route.gc\_elasticity = 9 net.ipv6.route.gc\_interval = 30 net.ipv6.route.gc\_min\_interval = 0 net.ipv6.route.gc\_min\_interval\_ms = 500 net.ipv6.route.gc\_thresh = 1024 net.ipv6.route.gc\_timeout = 60 net.ipv6.route.max\_size = 16384 net.ipv6.route.min\_adv\_mss = 1220 net.ipv6.route.mtu\_expires = 600 net.ipv6.xfrm6\_gc\_thresh = 32768 net.netfilter.nf\_conntrack\_acct = 0 net.netfilter.nf\_conntrack\_buckets = 16384 net.netfilter.nf\_conntrack\_checksum = 1 net.netfilter.nf\_conntrack\_count = 4 net.netfilter.nf\_conntrack\_dccp\_loose = 1 net.netfilter.nf\_conntrack\_dccp\_timeout\_closereq = 64 net.netfilter.nf\_conntrack\_dccp\_timeout\_closing = 64 net.netfilter.nf\_conntrack\_dccp\_timeout\_open = 43200 net.netfilter.nf\_conntrack\_dccp\_timeout\_partopen = 480 net.netfilter.nf\_conntrack\_dccp\_timeout\_request = 240 net.netfilter.nf\_conntrack\_dccp\_timeout\_respond = 480 net.netfilter.nf\_conntrack\_dccp\_timeout\_timewait = 240 net.netfilter.nf\_conntrack\_events = 1 net.netfilter.nf\_conntrack\_events\_retry\_timeout = 15 net.netfilter.nf\_conntrack\_expect\_max = 256 net.netfilter.nf\_conntrack\_frag6\_high\_thresh = 4194304 net.netfilter.nf\_conntrack\_frag6\_low\_thresh = 3145728 net.netfilter.nf\_conntrack\_frag6\_timeout = 60 net.netfilter.nf\_conntrack\_generic\_timeout = 600 net.netfilter.nf\_conntrack\_helper = 1 net.netfilter.nf\_conntrack\_icmp\_timeout = 30 net.netfilter.nf\_conntrack\_icmpv6\_timeout = 30 net.netfilter.nf\_conntrack\_log\_invalid = 0 net.netfilter.nf\_conntrack\_max = 65536 net.netfilter.nf\_conntrack\_sctp\_timeout\_closed = 10 net.netfilter.nf\_conntrack\_sctp\_timeout\_cookie\_echoed = 3 net.netfilter.nf\_conntrack\_sctp\_timeout\_cookie\_wait = 3 net.netfilter.nf\_conntrack\_sctp\_timeout\_established = 432000 net.netfilter.nf\_conntrack\_sctp\_timeout\_heartbeat\_acked = 210 net.netfilter.nf\_conntrack\_sctp\_timeout\_heartbeat\_sent = 30 net.netfilter.nf\_conntrack\_sctp\_timeout\_shutdown\_ack\_sent = 3 net.netfilter.nf\_conntrack\_sctp\_timeout\_shutdown\_recd = 0 net.netfilter.nf\_conntrack\_sctp\_timeout\_shutdown\_sent = 0 net.netfilter.nf\_conntrack\_tcp\_be\_liberal = 0 net.netfilter.nf\_conntrack\_tcp\_loose = 1 net.netfilter.nf\_conntrack\_tcp\_max\_retrans = 3 net.netfilter.nf\_conntrack\_tcp\_timeout\_close = 10 net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait = 60 net.netfilter.nf\_conntrack\_tcp\_timeout\_established = 432000 net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait = 120 net.netfilter.nf\_conntrack\_tcp\_timeout\_last\_ack = 30 net.netfilter.nf\_conntrack\_tcp\_timeout\_max\_retrans = 300 net.netfilter.nf\_conntrack\_tcp\_timeout\_syn\_recv = 60 net.netfilter.nf\_conntrack\_tcp\_timeout\_syn\_sent = 120 net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait = 120 net.netfilter.nf\_conntrack\_tcp\_timeout\_unacknowledged = 300 net.netfilter.nf\_conntrack\_timestamp = 0 net.netfilter.nf\_conntrack\_udp\_timeout = 30 net.netfilter.nf\_conntrack\_udp\_timeout\_stream = 180 net.netfilter.nf\_log.0 = NONE net.netfilter.nf\_log.1 = NONE net.netfilter.nf\_log.10 = NONE net.netfilter.nf\_log.11 = NONE net.netfilter.nf\_log.12 = NONE net.netfilter.nf\_log.2 = NONE net.netfilter.nf\_log.3 = NONE net.netfilter.nf\_log.4 = NONE net.netfilter.nf\_log.5 = NONE net.netfilter.nf\_log.6 = NONE net.netfilter.nf\_log.7 = NONE net.netfilter.nf\_log.8 = NONE net.netfilter.nf\_log.9 = NONE net.netfilter.nf\_log\_all\_netns = 0 net.nf\_conntrack\_max = 65536 net.unix.max\_dgram\_qlen = 512 user.max\_ipc\_namespaces = 7184 user.max\_mnt\_namespaces = 7184 user.max\_net\_namespaces = 7184 user.max\_pid\_namespaces = 7184 user.max\_user\_namespaces = 0 user.max\_uts\_namespaces = 7184 vm.admin\_reserve\_kbytes = 8192 vm.block\_dump = 0 vm.dirty\_background\_bytes = 0 vm.dirty\_background\_ratio = 10 vm.dirty\_bytes = 0 vm.dirty\_expire\_centisecs = 3000 vm.dirty\_ratio = 30 vm.dirty\_writeback\_centisecs = 500 vm.drop\_caches = 0 vm.extfrag\_threshold = 500 vm.hugepages\_treat\_as\_movable = 0 vm.hugetlb\_shm\_group = 0 vm.laptop\_mode = 0 vm.legacy\_va\_layout = 0 vm.lowmem\_reserve\_ratio = 256 256 32 vm.max\_map\_count = 65530 vm.memory\_failure\_early\_kill = 0 vm.memory\_failure\_recovery = 1 vm.min\_free\_kbytes = 45056 vm.min\_slab\_ratio = 5 vm.min\_unmapped\_ratio = 1 vm.mmap\_min\_addr = 4096 vm.mmap\_rnd\_bits = 28 vm.mmap\_rnd\_compat\_bits = 8 vm.nr\_hugepages = 0 vm.nr\_hugepages\_mempolicy = 0 vm.nr\_overcommit\_hugepages = 0 vm.nr\_pdflush\_threads = 0 vm.numa\_zonelist\_order = default vm.oom\_dump\_tasks = 1 vm.oom\_kill\_allocating\_task = 0 vm.overcommit\_kbytes = 0 vm.overcommit\_memory = 0 vm.overcommit\_ratio = 50 vm.page-cluster = 3 vm.panic\_on\_oom = 0 vm.percpu\_pagelist\_fraction = 0 vm.stat\_interval = 1 vm.swappiness = 30 vm.user\_reserve\_kbytes = 55257 vm.vfs\_cache\_pressure = 100 vm.zone\_reclaim\_mode = 0 |
| **加固方法** | 使用命令“vim /etc/sysctl.conf”修改配置文件，添加以下内容：  net.ipv4.icmp\_echo\_ignore\_broadcasts = 1 # 忽略ICMP广播  net.ipv4.icmp\_echo\_ignore\_all = 1 # 忽略ICMP echo请求  net.ipv4.ip\_default\_ttl = 128 # 修改TTL为128  使用命令“sysctl -p”使更改生效 |
| **加固结果** | 未加固，禁止ping会影响网络监控与故障排除 |
| **回退方案** | 使用命令“vim /etc/sysctl.conf”修改配置文件，注释掉以下内容：  net.ipv4.icmp\_echo\_ignore\_broadcasts = 1 # 忽略ICMP广播  net.ipv4.icmp\_echo\_ignore\_all = 1 # 忽略ICMP echo请求  net.ipv4.ip\_default\_ttl = 128 # 修改TTL为128  使用命令“sysctl -p”使更改生效 |
| **基线符合性**  **判定依据** | 系统忽略ICMP广播、忽略ICMP echo请求、TTL为128 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + 1. **文件系统**
       1. **重要目录和文件的权限设置**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-01-01** |
| **操作目的** | 合理配置重要目录和文件的权限，增强安全性 |
| **检查方法** | 执行以下命令检查目录和文件的权限设置情况：  chmod 700 /bin/rpm   chmod 600 /etc/exports  #NFS共享目录配置文件 chmod 600 /etc/hosts.\*  #主机访问控制文件 chmod 644 /var/log/messages #系统日志配置文件 chmod 640 /etc/syslog.conf chmod 660 /var/log/wtmp chmod 640 /var/log/lastlog chmod 600 /etc/ftpusers #用户口令文件 chmod 644 /etc/passwd chmod 600 /etc/shadow #校验模块配置文件目录 chmod R 750 /etc/pam.d  chmod 600 /etc/lilo.conf #终端配置文件 chmod 600 /etc/securetty chmod 400 /etc/shutdown.allow #系统访问安全配置文件 chmod 700 /etc/security #网络系统配置文件 chmod R 751 /etc/sysconfig #超级守护进程配置文件 chmod 600 /etc/xinetd.conf chmod 600 /etc/inetd.conf chmod -R 750 /etc/rc.d/init.d/ chmod 750 /etc/rc.d/init.d/\* #自动运行程序控制文件 chmod 600 /etc/crontab chmod 400 /etc/cron.\* #SSH配置文件 chmod 750 /etc/ssh #内核控制配置文件 chmod 400 /etc/sysctl.confg |
| **检查结果** | 是否符合：  不适用  现状：  -rwxr-xr-x. 1 root root 16128 10月 1 2020 /bin/rpm -rw-------. 1 root root 0 8月 9 2019 /etc/cron.deny -rw-r--r--. 1 root root 451 6月 10 2014 /etc/crontab -rw-r--r--. 1 root root 0 6月 7 2013 /etc/exports -rw-r--r--. 1 root root 370 6月 7 2013 /etc/hosts.allow -rw-r--r--. 1 root root 460 6月 7 2013 /etc/hosts.deny -rw-r--r--. 1 root root 846 9月 14 06:07 /etc/passwd -rw-r--r--. 1 root root 18281 5月 22 2020 /etc/rc.d/init.d/functions -rwxr-xr-x. 1 root root 4569 5月 22 2020 /etc/rc.d/init.d/netconsole -rwxr-xr-x. 1 root root 7928 5月 22 2020 /etc/rc.d/init.d/network -rw-r--r--. 1 root root 1160 2月 3 2021 /etc/rc.d/init.d/README -rw-------. 1 root root 221 4月 1 2020 /etc/securetty ----------. 1 root root 585 9月 14 06:07 /etc/shadow -rw-r--r--. 1 root root 292000 10月 14 10:20 /var/log/lastlog -rw-------. 1 root root 581709 10月 14 12:11 /var/log/messages -rw-rw-r--. 1 root utmp 11520 10月 14 10:20 /var/log/wtmp  /etc/cron.d: 总用量 16 drwxr-xr-x. 2 root root 21 9月 14 06:05 . drwxr-xr-x. 74 root root 8192 10月 14 10:19 .. -rw-r--r--. 1 root root 128 8月 9 2019 0hourly  /etc/cron.daily: 总用量 20 drwxr-xr-x. 2 root root 42 9月 14 06:05 . drwxr-xr-x. 74 root root 8192 10月 14 10:19 .. -rwx------. 1 root root 219 4月 1 2020 logrotate -rwxr-xr-x. 1 root root 618 10月 30 2018 man-db.cron  /etc/cron.hourly: 总用量 16 drwxr-xr-x. 2 root root 22 6月 10 2014 . drwxr-xr-x. 74 root root 8192 10月 14 10:19 .. -rwxr-xr-x. 1 root root 392 8月 9 2019 0anacron  /etc/cron.monthly: 总用量 12 drwxr-xr-x. 2 root root 6 6月 10 2014 . drwxr-xr-x. 74 root root 8192 10月 14 10:19 ..  /etc/cron.weekly: 总用量 12 drwxr-xr-x. 2 root root 6 6月 10 2014 . drwxr-xr-x. 74 root root 8192 10月 14 10:19 ..  /etc/pam.d: 总用量 112 drwxr-xr-x. 2 root root 4096 9月 13 22:13 . drwxr-xr-x. 74 root root 8192 10月 14 10:19 .. -rw-r--r--. 1 root root 192 2月 3 2021 chfn -rw-r--r--. 1 root root 192 2月 3 2021 chsh -rw-r--r--. 1 root root 232 4月 1 2020 config-util -rw-r--r--. 1 root root 287 8月 9 2019 crond lrwxrwxrwx. 1 root root 19 9月 14 06:07 fingerprint-auth -> fingerprint-auth-ac -rw-r--r--. 1 root root 702 9月 14 06:07 fingerprint-auth-ac -rw-r--r--. 1 root root 796 2月 3 2021 login -rw-r--r--. 1 root root 154 4月 1 2020 other -rw-r--r--. 1 root root 188 4月 1 2020 passwd lrwxrwxrwx. 1 root root 16 9月 14 06:07 password-auth -> password-auth-ac -rw-r--r--. 1 root root 1033 9月 14 06:07 password-auth-ac -rw-r--r--. 1 root root 155 4月 1 2020 polkit-1 lrwxrwxrwx. 1 root root 12 9月 14 06:07 postlogin -> postlogin-ac -rw-r--r--. 1 root root 330 9月 14 06:07 postlogin-ac -rw-r--r--. 1 root root 681 2月 3 2021 remote -rw-r--r--. 1 root root 143 2月 3 2021 runuser -rw-r--r--. 1 root root 138 2月 3 2021 runuser-l lrwxrwxrwx. 1 root root 17 9月 14 06:07 smartcard-auth -> smartcard-auth-ac -rw-r--r--. 1 root root 752 9月 14 06:07 smartcard-auth-ac lrwxrwxrwx. 1 root root 25 9月 14 06:05 smtp -> /etc/alternatives/mta-pam -rw-r--r--. 1 root root 76 4月 1 2020 smtp.postfix -rw-r--r--. 1 root root 904 8月 9 2019 sshd -rw-r--r--. 1 root root 540 2月 3 2021 su -rw-r--r--. 1 root root 200 1月 27 2021 sudo -rw-r--r--. 1 root root 178 1月 27 2021 sudo-i -rw-r--r--. 1 root root 137 2月 3 2021 su-l lrwxrwxrwx. 1 root root 14 9月 14 06:07 system-auth -> system-auth-ac -rw-r--r--. 1 root root 1031 9月 14 06:07 system-auth-ac -rw-r--r--. 1 root root 129 2月 3 2021 systemd-user -rw-r--r--. 1 root root 84 10月 31 2018 vlock  /etc/rc.d/init.d/: 总用量 40 drwxr-xr-x. 2 root root 70 9月 13 22:13 . drwxr-xr-x. 10 root root 127 11月 17 2020 .. -rw-r--r--. 1 root root 18281 5月 22 2020 functions -rwxr-xr-x. 1 root root 4569 5月 22 2020 netconsole -rwxr-xr-x. 1 root root 7928 5月 22 2020 network -rw-r--r--. 1 root root 1160 2月 3 2021 README  /etc/ssh: 总用量 616 drwxr-xr-x. 2 root root 225 9月 14 06:08 . drwxr-xr-x. 74 root root 8192 10月 14 10:19 .. -rw-r--r--. 1 root root 581843 8月 9 2019 moduli -rw-r--r--. 1 root root 2276 8月 9 2019 ssh\_config -rw-------. 1 root root 3907 8月 9 2019 sshd\_config -rw-r-----. 1 root ssh\_keys 227 9月 14 06:08 ssh\_host\_ecdsa\_key -rw-r--r--. 1 root root 162 9月 14 06:08 ssh\_host\_ecdsa\_key.pub -rw-r-----. 1 root ssh\_keys 387 9月 14 06:08 ssh\_host\_ed25519\_key -rw-r--r--. 1 root root 82 9月 14 06:08 ssh\_host\_ed25519\_key.pub -rw-r-----. 1 root ssh\_keys 1679 9月 14 06:08 ssh\_host\_rsa\_key -rw-r--r--. 1 root root 382 9月 14 06:08 ssh\_host\_rsa\_key.pub  /etc/sysconfig: 总用量 104 drwxr-xr-x. 6 root root 4096 9月 13 22:13 . drwxr-xr-x. 74 root root 8192 10月 14 10:19 .. -rw-r--r--. 1 root root 204 9月 14 06:07 anaconda -rw-r--r--. 1 root root 483 9月 14 06:07 authconfig drwxr-xr-x. 2 root root 43 9月 14 06:05 cbq -rw-r--r--. 1 root root 46 8月 8 2019 chronyd drwxr-xr-x. 2 root root 6 11月 17 2020 console -rw-r--r--. 1 root root 150 9月 7 23:00 cpupower -rw-------. 1 root root 110 8月 9 2019 crond -rw-------. 1 root root 1390 4月 11 2018 ebtables-config -rw-r--r--. 1 root root 73 4月 28 21:31 firewalld lrwxrwxrwx. 1 root root 15 9月 13 22:13 grub -> ../default/grub -rw-r--r--. 1 root root 798 11月 17 2020 init -rw-------. 1 root root 2134 10月 2 2020 ip6tables-config -rw-------. 1 root root 2116 10月 2 2020 iptables-config -rw-r--r--. 1 root root 903 8月 6 2019 irqbalance -rw-r--r--. 1 root root 1729 6月 10 00:09 kdump -rw-r--r--. 1 root root 180 9月 14 06:07 kernel -rw-r--r--. 1 root root 200 10月 30 2018 man-db drwxr-xr-x. 2 root root 6 11月 17 2020 modules -rw-r--r--. 1 root root 634 11月 17 2020 netconsole -rw-r--r--. 1 root root 22 9月 13 22:12 network drwxr-xr-x. 2 root root 4096 9月 13 22:13 network-scripts -rw-r--r--. 1 root root 15 8月 4 2017 rdisc -rw-r--r--. 1 root root 905 11月 17 2020 readonly-root -rw-r--r--. 1 root root 196 9月 30 2020 rsyslog -rw-r--r--. 1 root root 0 6月 10 2014 run-parts lrwxrwxrwx. 1 root root 17 9月 14 06:05 selinux -> ../selinux/config -rw-r-----. 1 root root 506 8月 9 2019 sshd -rw-r--r--. 1 root root 610 3月 16 2021 wpa\_supplicant |
| **加固方法** | 对于重要目录，建议执行如下类似操作：  chmod 700 /bin/rpm  chmod 600 /etc/exports  chmod 600 /etc/hosts.\*  chmod 644 /var/log/messages  chmod 640 /etc/syslog.conf  chmod 660 /var/log/wtmp  chmod 640 /var/log/lastlog  chmod 600 /etc/ftpusers  chmod 700 /bin/rpm  chmod 600 /etc/exports  chmod 600 /etc/hosts.\*  chmod 644 /var/log/messages  chmod 640 /etc/syslog.conf  chmod 660 /var/log/wtmp  chmod 640 /var/log/lastlog  chmod 600 /etc/ftpusers  chmod 644 /etc/passwd  chmod 600 /etc/shadow  chmod R 750 /etc/pam.d  chmod 600 /etc/lilo.conf  chmod 600 /etc/securetty  chmod 400 /etc/shutdown.allow  chmod 700 /etc/security  chmod -R 751 /etc/sysconfig  chmod 600 /etc/xinetd.conf  chmod 600 /etc/inetd.conf  chmod -R 750 /etc/rc.d/init.d/  chmod 750 /etc/rc.d/init.d/\*  chmod 600 /etc/crontab  chmod 400 /etc/cron.\*  chmod 750 /etc/ssh  chmod 400 /etc/sysctl.confg  这样只有root可以读、写和执行这个目录下的脚本。 |
| **加固结果** | 未加固 |
| **回退方法** | 使用 chmod命令将文件权限改回加固前权限 |
| **基线符合性**  **判定依据** | 重要目录只有root管理员具有读写权限。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **设置umask值**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-02-01** |
| **操作目的** | 设置默认的umask值，提高文件访问安全 |
| **检查方法** | 使用命令“umask”查看默认的umask值是否为027 |
| **检查结果** | 是否符合：  不符合  现状：  0022 |
| **加固方法** | 备份“cp /etc/profile /etc/profile.bak”  使用命令“vim /etc/profile”修改配置文件，添加行“umask 0027”， 即新创建的文件属主读写执行权限，同组用户读和执行权限，其他用户无权限，使用命令“umask 0027”应用设置 |
| **加固结果** | 未加固 |
| **回退方法** | 使用命令“vim /etc/profile”修改配置文件，修改行“umask 0022” |
| **基线符合性**  **判定依据** | umask值为0027 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **Bash历史命令**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-03-01** |
| **操作目的** | 设置Bash保留历史命令的条数，保护管理员命令行信息，防止信息泄露 |
| **检查方法** | 使用命令“cat /etc/profile|grep HISTSIZE=”和““cat /etc/profile|grep HISTFILESIZE=”查看保留历史命令的条数 |
| **检查结果** | 是否符合：  不符合  现状：  HISTSIZE=1000 |
| **加固结果** | 未加固 |
| **加固方法** | 使用命令“vim /etc/profile”修改配置文件，修改HISTSIZE=5和HISTFILESIZE=5即保留最新执行的5条命令 |
| **回退方法** | 使用命令“vim /etc/profile”修改配置文件，将HISTSIZE值改回1000 |
| **基线符合性**  **判定依据** | 执行histroy命令，保留历史命令的条数为5条 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **设置登录超时**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-04-01** |
| **操作目的** | 设置系统登录后，连接超时时间，增强安全性 |
| **检查方法** | 使用命令“cat /etc/profile |grep TMOUT”查看TMOUT是否被设置 |
| **检查结果** | 是否符合：  不符合  现状：  未配置 |
| **加固方法** | 使用命令“vim /etc/profile”修改配置文件，添加“TMOUT=”行开头的注释，设置为“TMOUT=300”，即超时时间为5分钟，使用“source /etc/profile”命令使之生效 |
| **加固结果** | 未加固 |
| **回退方法** | 使用命令“vim /etc/profile”修改配置文件，注释TMOUT行 |
| **基线符合性**  **判定依据** | 系统登录后用户5分钟时间空闲无输入后自动断开连接。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 管理员可以根据实际业务需要修改超时时间。 |

* + - 1. **检查root 路径**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-05-01** |
| **操作目的** | 确保root用户环境变量path中不包含“.”相对路径 |
| **检查方法** | root用户环境变量path中不应包含当前目录”.“  以root身份执行如下命令：  # echo $PATH  /usr/local/sbin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:. |
| **检查结果** | 是否符合：  符合  现状：  /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin |
| **加固方法** | 使用命令“vim /etc/profile”,去掉“.”。 |
| **加固结果** | 未加固，无需加固 |
| **回退方法** | 使用命令“vim /etc/profile”修改echo $PATH后面的路径，加上“.”。 |
| **基线符合性**  **判定依据** | Root用户环境变量中不能包含“.”相对路径。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **查找未授权的 SUID/SGID 文件**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-06-01** |
| **操作目的** | 查找未授权的 SUID/SGID |
| **检查方法** | 执行“find / -perm -04000;find / -perm -02000”命令，查找系统中所有的 SUID 和 SGID 程序。 |
| **检查结果** | 是否符合：  符合  现状：  /usr/bin/chfn /usr/bin/chsh /usr/bin/chage /usr/bin/gpasswd /usr/bin/newgrp /usr/bin/mount /usr/bin/su /usr/bin/sudo /usr/bin/umount /usr/bin/pkexec /usr/bin/crontab /usr/bin/passwd /usr/sbin/unix\_chkpwd /usr/sbin/pam\_timestamp\_check /usr/sbin/usernetctl /usr/lib/polkit-1/polkit-agent-helper-1 /usr/libexec/dbus-1/dbus-daemon-launch-helper /run/log/journal /run/log/journal/a02e2eb0c97f4322a52ada8bbb0a8be1 /usr/bin/wall /usr/bin/write /usr/bin/ssh-agent /usr/sbin/netreport /usr/sbin/postdrop /usr/sbin/postqueue /usr/libexec/utempter/utempter /usr/libexec/openssh/ssh-keysign |
| **加固方法** | 执行命令: find /usr/bin/chfn /usr/bin/chsh /usr/bin/passwd /usr/bin/su /usr/bin/chage /usr/bin/gpasswd /usr/bin/wall /usr/bin/chfn /usr/bin/chsh /usr/bin/newgrp /usr/bin/write /usr/sbin/usernetctl /usr/sbin/traceroute /bin/mount /bin/umount /bin/ping /sbin/netreport -type f -perm 6000 2>/dev/null 如果存在输出结果，则使用chmod 755 文件名 命令修改文件的权限。 例如：chmod a-s /usr/bin/chage |
| **加固结果** | 无需加固 |
| **回退方法** | 不需要回退 |
| **基线符合性**  **判定依据** | /usr/bin/chfn /usr/bin/chsh /usr/bin/passwd /usr/bin/su /usr/bin/chage /usr/bin/gpasswd /usr/bin/wall /usr/bin/chfn /usr/bin/chsh /usr/bin/newgrp /usr/bin/write /usr/sbin/usernetctl /usr/sbin/traceroute /bin/mount /bin/umount /bin/ping /sbin/netreport等文件符合6000权限。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 建议经常性的对比 suid/sgid 文件列表，以便能够及时发现可  疑的后门程序。 |

* + - 1. **不存在任何人都有写权限的目录**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-07-01** |
| **操作目的** | 检查任何人都有写权限的目录，确保文件系统安全 |
| **检查方法** | 在系统中定位任何人都有写权限的目录用下面的命令：  for PART in `awk '($3 == "ext2" || $3 == "ext3") \  { print $2 }' /etc/fstab`; do  find $PART -xdev -type d \( -perm -0002 -a ! -perm -1000  \) -print  Done |
| **检查结果** | 是否符合：  符合  现状：  未找到 |
| **加固方法** | 使用“chmod + 相应权限 + 文件/目录”修改目录权限。 |
| **加固结果** | 未加固 |
| **回退方法** | 不需要回退 |
| **基线符合性**  **判定依据** | 若命令返回值非空，则低于安全要求。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **查找任何人都有写权限的文件**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-08-01** |
| **操作目的** | 查找任何人都有写权限的文件，确保文件系统安全 |
| **检查方法** | 在系统中定位任何人都有写权限的文件用下面的命令：  for PART in `grep -v ^# /etc/fstab | awk '($6 != "0")  {print $2 }'`; do  find $PART -xdev -type f \( -perm -0002 -a ! -perm -1000  \) -print  Done |
| **检查结果** | 是否符合：  符合  现状：  未找到 |
| **加固方法** | 使用“chmod + 相应权限 + 文件/目录”修改文件权限。 |
| **加固结果** | 未加固 |
| **回退方法** | 不需要回退 |
| **基线符合性**  **判定依据** | 若命令返回值非空，则低于安全要求。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **检查没有属主的文件**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-09-01** |
| **操作目的** | 检查没有属主的文件，确保文件系统安全 |
| **检查方法** | 定位系统中没有属主的文件用下面的命令：  for PART in `grep -v ^# /etc/fstab | awk '($6 != "0")  {print $2 }'`; do  find $PART -nouser -o -nogroup -print  done  注意：不用管“ /dev”目录下的那些文件 |
| **检查结果** | 是否符合：  符合  现状：  未找到 |
| **加固方法** | 删除没有属主的文件。 |
| **加固结果** | 未加固 |
| **回退方法** | 不需要回退 |
| **基线符合性**  **判定依据** | 若命令返回值非空，则低于安全要求。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + - 1. **检查异常隐含文件**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-06-10-01** |
| **操作目的** | 检查异常隐含文件，确保文件系统安全 |
| **检查方法** | 用“find”程序可以查找到这些隐含文件。例如：  find / -name ".. \*" -print –xdev  find / -name " ⋯ \*" -print -xdev | cat -v  同时也要注意象“.xx”和“ .mail ”这样的文件名的。 （这  些文件名看起来都很像正常的文件名） |
| **检查结果** | 是否符合：  符合  现状：  未找到 |
| **加固方法** | 删除异常隐含文件 |
| **加固结果** | 未加固，无需加固 |
| **回退方法** | 不需要回退 |
| **基线符合性**  **判定依据** | 若命令返回值非空，则低于安全要求。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** |  |

* + 1. **日志**
       1. **Syslogd认证相关记录**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-07-01-01** |
| **操作目的** | 查看登录认证日志，确保身份认证权限安全 |
| **检查方法** | cat /etc/rsyslog.conf |grep authpriv  查看是否有authpriv.\* /var/log/secure |
| **检查结果** | 是否符合：  符合  现状：  \*.info;mail.none;authpriv.none;cron.none /var/log/messages # The authpriv file has restricted access. authpriv.\* /var/log/secure |
| **加固方法** | 添加相关日志的记录：  将authpirv设备的任何级别的信息记录到/var/log/secure 文件中 |
| **加固结果** | 未加固 |
| **回退方法** | vim编辑/etc/rsyslog.conf，注释authpriv行 |
| **基线符合性**  **判定依据** | 应对所有系统登录认证事件在/var/log/secure中进行记录。 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | authpirv主要是认证、权限使用相关的信息。 |

* + - 1. **syslogd日志设置**

|  |  |
| --- | --- |
| **编号** | **SEC-Linux-v1.0-07-02-01** |
| **操作目的** | 查看所有日志记录 |
| **检查方法** | 使用命令“cat /etc/rsyslog.conf”查看syslogd的配置  系统日志（默认）/var/log/messages  cron日志（默认）/var/log/cron  安全日志（默认）/var/log/secure |
| **检查结果** | 是否符合：  符合  现状：  # rsyslog configuration file  # For more information see /usr/share/doc/rsyslog-\*/rsyslog\_conf.html # If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html  #### MODULES ####  # The imjournal module bellow is now used as a message source instead of imuxsock. $ModLoad imuxsock # provides support for local system logging (e.g. via logger command) $ModLoad imjournal # provides access to the systemd journal #$ModLoad imklog # reads kernel messages (the same are read from journald) #$ModLoad immark # provides --MARK-- message capability  # Provides UDP syslog reception #$ModLoad imudp #$UDPServerRun 514  # Provides TCP syslog reception #$ModLoad imtcp #$InputTCPServerRun 514   #### GLOBAL DIRECTIVES ####  # Where to place auxiliary files $WorkDirectory /var/lib/rsyslog  # Use default timestamp format $ActionFileDefaultTemplate RSYSLOG\_TraditionalFileFormat  # File syncing capability is disabled by default. This feature is usually not required, # not useful and an extreme performance hit #$ActionFileEnableSync on  # Include all config files in /etc/rsyslog.d/ $IncludeConfig /etc/rsyslog.d/\*.conf  # Turn off message reception via local log socket; # local messages are retrieved through imjournal now. $OmitLocalLogging on  # File to store the position in the journal $IMJournalStateFile imjournal.state   #### RULES ####  # Log all kernel messages to the console. # Logging much else clutters up the screen. #kern.\* /dev/console  # Log anything (except mail) of level info or higher. # Don't log private authentication messages! \*.info;mail.none;authpriv.none;cron.none /var/log/messages  # The authpriv file has restricted access. authpriv.\* /var/log/secure  # Log all the mail messages in one place. mail.\* -/var/log/maillog   # Log cron stuff cron.\* /var/log/cron  # Everybody gets emergency messages \*.emerg :omusrmsg:\*  # Save news errors of level crit and higher in a special file. uucp,news.crit /var/log/spooler  # Save boot messages also to boot.log local7.\* /var/log/boot.log   # ### begin forwarding rule ### # The statement between the begin ... end define a SINGLE forwarding # rule. They belong together, do NOT split them. If you create multiple # forwarding rules, duplicate the whole block! # Remote Logging (we use TCP for reliable delivery) # # An on-disk queue is created for this action. If the remote host is # down, messages are spooled to disk and sent when it is up again. #$ActionQueueFileName fwdRule1 # unique name prefix for spool files #$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible) #$ActionQueueSaveOnShutdown on # save messages to disk on shutdown #$ActionQueueType LinkedList # run asynchronously #$ActionResumeRetryCount -1 # infinite retries if host is down # remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional #\*.\* @@remote-host:514 # ### end of the forwarding rule ### |
| **加固方法** | vim /etc/rsyslog.conf打开日志配置文件，增加如下日志配置：  # Don't log private authentication messages!  \*.info;mail.none;authpriv.none;cron.none /var/log/messages  # The authpriv file has restricted access.  authpriv.\* /var/log/secure  # Log cron stuff  cron.\* /var/log/cron  # 外部日志服务器配置，将日志传输到日志服务器  \*.\* @@X.X.103.61:514;RSYSLOG\_SyslogProtocol23Form |
| **加固结果** | 未加固 |
| **回退方法** | vim编辑/etc/syslog.conf，注释加固中添加的日志记录，或改回加固前相应日志记录的等级。 |
| **基线符合性**  **判定依据** | 开启日志服务，并传输到外部日志服务器 |
| **适用版本** | CentOS 6、CentOS 7、RedHat 6、RedHat 7 |
| **备注** | 建议通过Graylog搭建集中日志系统 |