

CentOS/RedHat Tips

?????????

CentOS 7/8: secure-linux.sh

```
#!/usr/bin/env bash
# Author: A.Lang(alang.hsu[AT]gmail.com)
# File: secure-linux.sh
# Created by 2019/3/1
#
#
SVC_LIST=""
##### Start #####
#
## bluetooth services
bluetooth

## SELinux
auditd

## Disk Monitoring
smartd

## Linux Virtualization with KVM
libvirt

## ABRT - Automatic Bug Reporting Tool
abrt
abrt-ccpp

## More Services
firewalld
avahi-daemon
#chronyd
cups
```

```

autofs
#
#
##### End #####
"

# function report_result <service name> <status>
report_result() {
    printf "%20s .....%s\n" "$1" "$2"
}

## Main program
#echo "$SVC_LIST" | sed -e '/^#/d' -e '/^$/d'
echo
echo "The following services will be disabled:"
echo "$SVC_LIST" | sed -e '/^#/d' -e '/^$/d' | while read name
do
    chkconfig $line off 2>/dev/null
    systemctl disable $name 2>/dev/null
    if [ $? -eq 0 ]; then
        report_result $name "OK"
    else
        report_result $name "***"
    fi
done

## Disable SELinux
SVC="SELinux"
sed -i 's/SELINUX=.*$/SELINUX=disabled/' /etc/selinux/config 2>/dev/null
if [ $? -eq 0 ]; then
    report_result $SVC "OK"
else
    report_result $SVC "***"
fi

echo "All done, please reboot NOW."

```

CentOS 6: secure-linux.sh

```
#!/usr/bin/env bash
# Author: A.Lang(alang.hsu[AT]gmail.com)
# File: secure-linux.sh
# Created by 2011-11-27
# Updated by 2016-11-2
#
SVC_LIST=""
##### Start #####
#
## Disable if the system is ACPI capable
apmd

## bluetooth services
bluetooth
hidd

## IR device
irda

## only needed the first time a system is configured
firstboot
readahead_early

## SELinux
auditd
setroubleshoot

## Disk Monitoring
smartd

## More Services
anacron
avahi-daemon
avahi-daemon
cups
isdn
ip6tables
iptables
iscsi
```

```

iscsid
mcstrans
pcscd
autofs
yum-updatesd
NetworkManager
#
#
##### End #####
"

# function report_result <service name> <status>
report_result() {
    printf "%20s .....%s\n" "$1" "$2"
}

## Main program
#echo "$SVC_LIST" | sed -e '/^#/d' -e '/^$/d'
echo
echo "The following services will be disabled:"
echo "$SVC_LIST" | sed -e '/^#/d' -e '/^$/d' | while read line
do
    chkconfig $line off 2>/dev/null
    if [ $? -eq 0 ]; then
        report_result $line "OK"
    else
        report_result $line "***"
    fi
done

## Disable SELinux
SVC="SELinux"
sed -i 's/SELINUX=.*$/SELINUX=disabled/' /etc/selinux/config 2>/dev/null
if [ $? -eq 0 ]; then
    report_result $SVC "OK"
else
    report_result $SVC "***"
fi

```

```
echo "All done, please reboot NOW."
```

Remove virbr0 network interface

Case 1: Not using libvirtd service and virbr0 interface

```
# Stop and Disable the service
systemctl stop libvirtd.service
systemctl disable libvirtd.service

# Reboot the host to remove the virbr0 interface
systemctl reboot
```

Case 2: Using libvirtd and dont want "virbr0"

```
# List the default network set-up for the virtual machines
virsh net-list

Name      State   Autostart   Persistent
-----
default   active  yes         yes

# Destroy the network default.
virsh net-destroy default

Network default destroyed

# Permanently remove the default virtual network from the configuration.
virsh net-undefine default

Network default has been undefined

# The interface virbr0 is now gone. You can verify it in the ifconfig or ip command output.
ifconfig virbr0

virbr0: error fetching interface information: Device not found
```

Case 3: Removing virbr0 interface on running machines (non-persistence across reboots)

First, list out the virtual bridge interfaces available on the system using the below command.

```
brctl show
```

bridge name	bridge id	STP enabled	interfaces
virbr0	8000.5254003008b6	yes	virbr0-nic

Make the bridge interface down before removal.

```
ip link set virbr0 down
```

Now, remove the bridge

```
brctl delbr virbr0
```

check if the bridge is removed

```
brctl show
```

bridge name	bridge id	STP enabled	interfaces
-------------	-----------	-------------	------------

Removing lxcbr0 interface

change the below line in /etc/sysconfig/lxc. This will be effective after reboot. change the line from

```
USE_LXC_BRIDGE="true"
```

to

```
USE_LXC_BRIDGE="false"
```

remove the lxcbr0 bridge interface for the running system

```
brctl show
```

```
ip link set lxcbr0 down
```

```
brctl delbr lxcbr0
```

```
brctl show
```

New Changes to RedHat 9

Official: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/considerations_in_adopting_rhel_9/assembly_security_considerations-in-adopting-rhel-9

1. [SSH from RHEL 9 to RHEL 6 systems does not work](#)

- The following algorithms are disabled in the LEGACY, DEFAULT and FUTURE crypto policies provided with RHEL 9:
 - TLS older than version 1.2 (since RHEL 9, was < 1.0 in RHEL 8)
 - DTLS older than version 1.2 (since RHEL 9, was < 1.0 in RHEL 8)
 - DH with parameters < 2048 bits (since RHEL 9, was < 1024 bits in RHEL 8)
 - RSA with key size < 2048 bits (since RHEL 9, was < 1024 bits in RHEL 8)
 - DSA (since RHEL 9, was < 1024 bits in RHEL 8)
 - 3DES (since RHEL 9)
 - RC4 (since RHEL 9)
 - FFDHE-1024 (since RHEL 9)
 - DHE-DSS (since RHEL 9)
 - Camellia (since RHEL 9)
 - ARIA
 - SEED
 - IDEA
 - Integrity-only cipher suites
 - TLS CBC mode cipher suites using SHA-384 HMAC
 - AES-CCM8
 - All ECC curves incompatible with TLS 1.3, including secp256k1
 - IKEv1 (since RHEL 8)
- SCP not supported in RHEL 9
- OpenSSH root password login disabled by default
- GnuTLS no longer supports TPM 1.2
- Support for disabling SELinux through `/etc/selinux/config` has been removed. If your scenario requires disabling SELinux, add the `selinux=0` parameter to your kernel command line.
- Network **teams** are deprecated
- RHEL 9 does not contain the `network-scripts` package that provided the deprecated legacy network scripts in RHEL 8. To configure network connections in RHEL 9, use **NetworkManager**.

sosreport ??????

[illegible]

?????

```
# [REDACTED] sosreport [REDACTED]
yum install sos

# [REDACTED]
#sosreport

# NOTE: [REDACTED] /tmp[REDACTED] sosreport-*.tar.bz2 [REDACTED]
# Updated by 2023/2/1

# [REDACTED] RHEL 8 [REDACTED] sosreport[REDACTED] /var/tmp[REDACTED]
```

```

sos report

# [redacted] /tmp [redacted]

sos report --tmp-dir /path/to/directory

## [redacted]

# [redacted] plugins

sos report -l

# [redacted] plugins [redacted]

sos report -n kvm,amd

```

“ sosreport ???????? <https://access.redhat.com/solutions/3592> ?

??????????

- ???????? sos_reports ??? sosreport.html ??????????????????????????????
- [xsos](#) - Github ???

- ???????? sos_reports ???? sosreport.html ??????????????????????????????
- [xsos](#) - Github ???

RedHat Linux ????

- [What are RHEL in-place upgrades? \(redhat.com\)](#)

- [What are RHEL in-place upgrades? \(redhat.com\)](https://www.redhat.com/en/what-is-rhel-in-place-upgrade)

FAQ

setlocale error

setlocale error

```
“ -bash: warning: setlocale: LC_CTYPE: cannot change locale (zh_TW.big5):  
No such file or directory  
-bash: warning: setlocale: LC_CTYPE: cannot change locale (zh_TW.big5):  
No such file or directory
```

```
“ -bash: warning: setlocale: LC_CTYPE: cannot change locale (zh_TW.big5):  
No such file or directory  
-bash: warning: setlocale: LC_CTYPE: cannot change locale (zh_TW.big5):  
No such file or directory
```

?????????? zh_TW.big5

```
locale -a | grep zh_TW.big5
```

```
locale -a | grep zh_TW.big5
```

??????????


```
yum install glibc-all-langpacks.x86_64
```

????????????

RHEL8: Stopping the message when ssh login to the host

“ Activate the web console with: `systemctl enable --now cockpit.socket`

Solution:

```
ln -sf /dev/null /etc/motd.d/cockpit
```

Systemd messages: Created slice, Starting Session

????? /var/log/messages ????????????

“ Jul 24 08:50:01 example.com systemd: Created slice user-0.slice.
Jul 24 08:50:01 example.com systemd: Starting Session 150 of user root.
Jul 24 08:50:01 example.com systemd: Started Session 150 of user root.
Jul 24 09:00:01 example.com systemd: Created slice user-0.slice.
Jul 24 09:00:02 example.com systemd: Starting Session 151 of user root.
Jul 24 09:00:02 example.com systemd: Started Session 151 of user root.

?? Cron job ??? [Logs flooded with systemd messages: Created slice, Starting Session - Red Hat Customer Portal](#)

?????????(suppress)?? rsyslog????????

```
echo 'if $programname == "systemd" and ($msg contains "Starting Session" or $msg contains "Started Session" or $msg contains "Created slice" or $msg contains "Starting user-" or $msg contains "Starting User Slice of" or $msg contains "Removed session" or $msg contains "Removed slice User Slice of" or $msg contains "Stopping User Slice of") then stop' >/etc/rsyslog.d/ignore-systemd-session-slice.conf
```

```
systemctl restart rsyslog
```

useradd errors

?? `useradd` ??????????????????????

“ [sss_cache] [sysdb_domain_cache_connect] (0x0010): DB version too old [0.23], expected [0.24] for domain implicit_files!
Higher version of database is expected!
In order to upgrade the database, you must run SSSD.
Removing cache files in /var/lib/sss/db should fix the issue, but note that removing cache files will also remove all of your cached credentials.
Could not open available domains

Solution:

- KB: <https://access.redhat.com/solutions/7031304>

```
systemctl stop sssd ; rm -f /var/lib/sss/db/* ; systemctl start sssd
```

Revision #36

Created 16 August 2020 03:51:50 by Admin

Updated 23 April 2025 10:19:36 by Admin