Fall2019 Cent OS 7 log operation

The presentation works with log files.

Preuss
12/5/2019

Cent OS 7 Settings on both systems

40 GB disk
8 GB RAM
2 Processors
NAT Network Settings

Software Install: Server with GUI (no additional software)
Automatic partitioning
No security policy chosen

Post-Installation
Install open-vm-tools
Install updates

Resource:
https://www.loggly.com/ultimate-guide/using-journalctl/
http://man7.org/linux/man-pages/man1/journalctl.1.html
http://man7.org/linux/man-pages/man5/journald.conf.5.html

log01 - VMware Workstation 15 Player (Non-commercial use only)

Player

Applications Places Fri 13:19

Home

Trash

The presentation logs into the system.

7
CENTOS

log01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 13:19

Home

Trash

preuss@log01:~

File Edit View Search Terminal Help

```
[preuss@log01 ~]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in the 'systemd-journal' group can see all messages. Pass -q to
      turn off this notice.
No journal files were opened due to insufficient permissions.
[preuss@log01 ~]$
```

The presentation tries running "journalctl".

preuss@log01:~

1 / 4

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
[preuss@log01 ~]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in the 'systemd-journal' group can see all messages. Pass -q to
      turn off this notice.
No journal files were opened due to insufficient permissions.
[preuss@log01 ~]$ su
Password:
[root@log01 preuss]# journalctl
```

The presentation runs "journalctl" as root.

log01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 13:20

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
-- Logs begin at Fri 2019-11-22 13:16:43 CST, end at Fri 2019-11-22 13:20:01 CST. --
Nov 22 13:16:43 log01.mait.minnesota.edu systemd-journal[95]: Runtime journal is using 8.0M (max allowed 390.1M, trying to leave 585.
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: Initializing cgroup subsys cpuset
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: Initializing cgroup subsys cpu
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: Initializing cgroup subsys cpuacct
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: Linux version 3.10.0-1062.4.3.el7.x86_64 (mockbuild@kbuilder.bsys.centos.org) (gcc v
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: Command line: BOOT_IMAGE=/vmlinuz-3.10.0-1062.4.3.el7.x86_64 root=/dev/mapper/centos
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: Disabled fast string operations
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: e820: BIOS-provided physical RAM map:
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009ebff] usable
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x000000000009ec00-0x000000000009ffff] reserved
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bfecffff] usable
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x00000000bfed0000-0x00000000bfefefff] ACPI data
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x0000
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x0000
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x0000
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x0000
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: BIOS-e820: [mem 0x0000
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: NX (Execute Disable) p
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: SMBIOS 2.7 present.
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: DMI: VMware, Inc. VMwa                                                    m, BIOS 6.0
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: Hypervisor detected: V
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: vmware: TSC freq read
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: vmware: Host bus clock
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: vmware: using sched of
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: e820: update [mem 0x00
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: e820: remove [mem 0x00
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: e820: last_pfn = 0x240000 max_arch_pfn = 0x400000000
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: MTRR default type: uncachable
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: MTRR fixed ranges enabled:
Nov 22 13:16:43 log01.mait.minnesota.edu kernel:   00000-9FFFF write-back
Nov 22 13:16:43 log01.mait.minnesota.edu kernel:   A0000-BFFFF uncachable
Nov 22 13:16:43 log01.mait.minnesota.edu kernel:   C0000-CBFFF write-protect
Nov 22 13:16:43 log01.mait.minnesota.edu kernel:   CC000-EFFFF uncachable
Nov 22 13:16:43 log01.mait.minnesota.edu kernel:   F0000-FFFFF write-protect
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: MTRR variable ranges enabled:
lines 1-39
```

This is a sample of the output of "journalctl". The presentation presses "Enter" to move to the next screen.

preuss@log01:/home/preuss

1 / 4

log01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 13:21

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
[root@log01 preuss]# journalctl -b
```

The presentation runs "journalctl -b" to see the boot log entries.

log01 - VMware Workstation 15 Player (Non-commercial use only)

Player

Applications Places Terminal Fri 13:21

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.1: [15ad:07a0] type 01 class 0x060400
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.1: PME# supported from D0 D3hot D3cold
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.1: System wakeup disabled by ACPI
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.2: [15ad:07a0] type 01 class 0x060400
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.2: PME# supported from D0 D3hot D3cold
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.2: System wakeup disabled by ACPI
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.3: [15ad:07a0] type 01 class 0x060400
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.3: PME# supported from D0 D3hot D3cold
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.3: System wakeup disabled by ACPI
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.4: [15ad:07a0] type 01 class 0x060400
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.4: PME# supported from D0 D3hot D3cold
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.4: System wakeup disabled by ACPI
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.5: [15ad:07a0] type 01 class 0x060400
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.5: PME# supported from D0 D3hot D3cold
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.5: System w
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.6: [15ad:07
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.6: PME# sup
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.6: System w
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.7: [15ad:07
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.7: PME# sup
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:17.7: System w
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.0: [15ad:07
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.0: PME# sup
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.0: System w
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.1: [15ad:07
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.1: PME# sup
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.1: System w
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.2: [15ad:07
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.2: PME# sup
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.2: System w
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.3: [15ad:07
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.3: PME# supported from D0 D3hot D3cold
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.3: System wakeup disabled by ACPI
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.4: [15ad:07a0] type 01 class 0x060400
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.4: PME# supported from D0 D3hot D3cold
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.4: System wakeup disabled by ACPI
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.5: [15ad:07a0] type 01 class 0x060400
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.5: PME# supported from D0 D3hot D3cold
Nov 22 13:16:43 log01.mait.minnesota.edu kernel: pci 0000:00:18.5: System wakeup disabled by ACPI
[root@log01 preuss]#
```

This is sample boot log entries.

preuss@log01:/home/preuss

1 / 4

log01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 13:22

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
[root@log01 preuss]# journalctl --list-boots
 0 e20d0c737de548a491d90e16f0a52b92 Fri 2019-11-22 13:16:43 CST—Fri 2019-11-22 13:20:44 CST
[root@log01 preuss]#
```

Home

Trash

The presentation runs "journalctl --list-boots" to see system boots.

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
[root@log01 preuss]# journalctl --list-boots
 0 e20d0c737de548a491d90e16f0a52b92 Fri 2019-11-22 13:16:43 CST—Fri 2019-11-22 13:20:44 CST
[root@log01 preuss]# journalctl -u yum
-- No entries --
[root@log01 preuss]#
```

The presentation runs "journalctl -u yum" to find any yum entries in journalctl.

log01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 13:24

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
[root@log01 preuss]# id preuss
uid=1000(preuss) gid=1000(preuss) groups=1000(preuss)
[root@log01 preuss]# journalctl _UID=1000
```

The presentation runs "id preuss" to get the UID of the login preuss.

The presentation runs "journalctl _UID=1000" to get login entries associated with the login preuss.

log01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 13:25

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
Nov 22 13:17:08 log01.mait.minnesota.edu gnome-session-binary[9041]: WARNING: App 'spice-vdagent.desktop' exited with code 1
Nov 22 13:17:08 log01.mait.minnesota.edu vmware-user.desktop[10767]: vmware-user: could not open /proc/fs/vmblock/dev
Nov 22 13:17:08 log01.mait.minnesota.edu spice-streaming-agent[10775]: Failed to open the streaming device "/dev/virtio-ports/org.spi
Nov 22 13:17:08 log01.mait.minnesota.edu vmtoolsd[10769]: gtk_disable_setlocale() must be called before gtk_init()
Nov 22 13:17:08 log01.mait.minnesota.edu org.gnome.Shell.desktop[9286]: Window manager warning: "XF86RFKill" is not a valid accelerat
Nov 22 13:17:08 log01.mait.minnesota.edu gsd-color[10607]: failed to get edid: unable to get EDID for output
Nov 22 13:17:08 log01.mait.minnesota.edu gnome-shell[9286]: Error looking up permission: GDBus.Error:org.freedesktop.portal.Error.Not
Nov 22 13:17:08 log01.mait.minnesota.edu gnome-session-binary[9041]: Entering running state
Nov 22 13:17:08 log01.mait.minnesota.edu tracker-store.desktop[10846]: (uint32 1,)
Nov 22 13:17:08 log01.mait.minnesota.edu libcanberra-login-sound.desktop[10811]: Failed to play sound: File or data not found
Nov 22 13:17:09 log01.mait.minnesota.edu com.redhat.imsettings[9051]: No such schema “org.gnome.settings-daemon.plugins.keyboard”
Nov 22 13:17:09 log01.mait.minnesota.edu imsettings-start.desktop[10823]: Current desktop isn't supported by IMSettings. Please follo
Nov 22 13:17:09 log01.mait.minnesota.edu gnome-shell[9286]: STACK_OP_
Nov 22 13:17:09 log01.mait.minnesota.edu gnome-shell[9286]: STACK_OP_
Nov 22 13:17:09 log01.mait.minnesota.edu gnome-shell[9286]: GNOME She                                                    ST)
Nov 22 13:17:09 log01.mait.minnesota.edu gsd-color[10607]: unable to                                                    r output
Nov 22 13:17:09 log01.mait.minnesota.edu gnome-software[10796]: plugi
Nov 22 13:17:10 log01.mait.minnesota.edu gnome-software[10796]: not G                                                   ark:1: Key fi
Nov 22 13:17:10 log01.mait.minnesota.edu gnome-software[10796]: enabl                                                   packagekit-lo
Nov 22 13:17:10 log01.mait.minnesota.edu gnome-software[10796]: disab                                                    epiphany, re
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: place                                                   known type 3
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: top-i                                                   own type 3
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: apps-                                                   own type 3
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: launc                                                   b.com unknown
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: alter                                                   unknown type
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: windo                                                   known type 3
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: Only
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: hidin                                                   ly 0 to show,
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: hiding category audio-video featured applications: found only 0 to sh
Nov 22 13:17:11 log01.mait.minnesota.edu gnome-software[10796]: Only 5 apps for popular list, hiding
Nov 22 13:17:12 log01.mait.minnesota.edu telepathy-haze[10319]: Exiting
Nov 22 13:17:40 log01.mait.minnesota.edu gnome-shell[9286]: JS WARNING: [resource:///org/gnome/shell/ui/workspaceThumbnail.js 891]: r
Nov 22 13:17:40 log01.mait.minnesota.edu gsd-color[10607]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Nov 22 13:17:40 log01.mait.minnesota.edu gsd-color[10607]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Nov 22 13:20:01 log01.mait.minnesota.edu su[11221]: (to root) preuss on pts/0
Nov 22 13:20:01 log01.mait.minnesota.edu su[11221]: pam_unix(su:session): session opened for user root by preuss(uid=1000)
Nov 22 13:20:44 log01.mait.minnesota.edu pulseaudio[9404]: [alsa-sink-ES1371/1] alsa-sink.c: ALSA woke us up to write new data to the
Nov 22 13:20:44 log01.mait.minnesota.edu pulseaudio[9404]: [alsa-sink-ES1371/1] alsa-sink.c: Most likely this is a bug in the ALSA dr
Nov 22 13:20:44 log01.mait.minnesota.edu pulseaudio[9404]: [alsa-sink-ES1371/1] alsa-sink.c: We were woken up with POLLOUT set -- how
lines 24-62/62 (END)
```

This is sample output of log events dealing with the preuss login.

preuss@log01:/home/preuss

1 / 4

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
[root@log01 preuss]# less /etc/systemd/journald.conf
```

The presentation reviews the journalclt configuration file.

Home

Trash

preuss@log01:/home/preuss

File Edit View Search Terminal Help

```
#  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.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See journald.conf(5) for details.

[Journal]
#Storage=auto
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
#RateLimitInterval=30s
#RateLimitBurst=1000
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize=
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
/etc/systemd/journald.conf
```

This is a partial listing of a journctl.conf file.