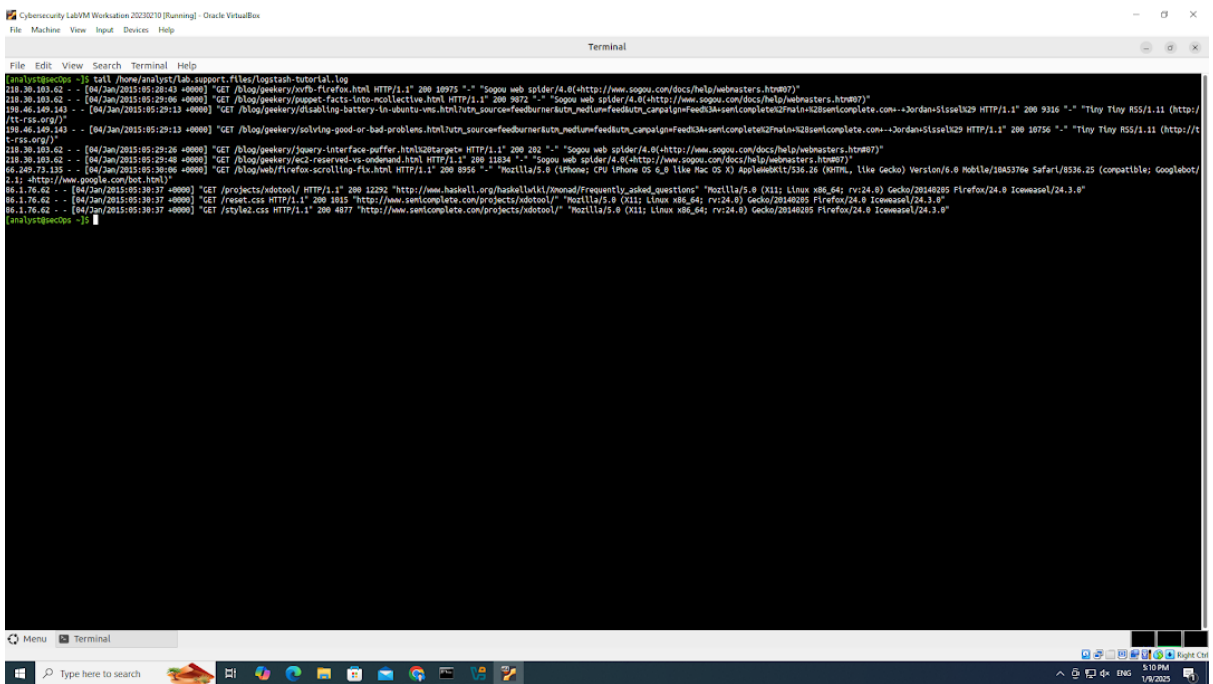


```
less /home/analyst/lab.support.files/logstash-tutorial.log
```



```

[analyst@secOps ~]$ sudo tail -f /home/analyst/lab.support.files/logstash-tutorial.log
[info] password for analyst:
210.30.103.62 - - [04/Jan/2015:05:20:43 +0000] "GET /blog/geekery/nvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(http://www.sogou.com/docs/help/webmasters.htm#077)"
210.30.103.62 - - [04/Jan/2015:05:20:06 +0000] "GET /blog/geekery/supnet-facts-into-collective.html HTTP/1.1" 200 9072 "-" "Sogou web spider/4.0(http://www.sogou.com/docs/help/webmasters.htm#077)"
190.46.149.143 - - [04/Jan/2015:05:20:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html HTTP/1.1" 200 10534 "-" "Sogou web spider/4.0(http://www.sogou.com/docs/help/webmasters.htm#077)"
190.46.149.143 - - [04/Jan/2015:05:20:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html HTTP/1.1" 200 10756 "-" "TINY Tiny RSS/1.11 (http://tiny-tiny.com/)"
210.30.103.62 - - [04/Jan/2015:05:20:26 +0000] "GET /blog/geekery/zoomy-interface-puffer.html HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(http://www.sogou.com/docs/help/webmasters.htm#077)"
210.30.103.62 - - [04/Jan/2015:05:20:28 +0000] "GET /blog/geekery/ed-reserved-ss-demand.html HTTP/1.1" 200 10534 "-" "Sogou web spider/4.0(http://www.sogou.com/docs/help/webmasters.htm#077)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/ndotool/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Monad/frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 IcoWassel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semanticcomplete.com/projects/ndotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 IcoWassel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semanticcomplete.com/projects/ndotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 IcoWassel/24.3.0"

```

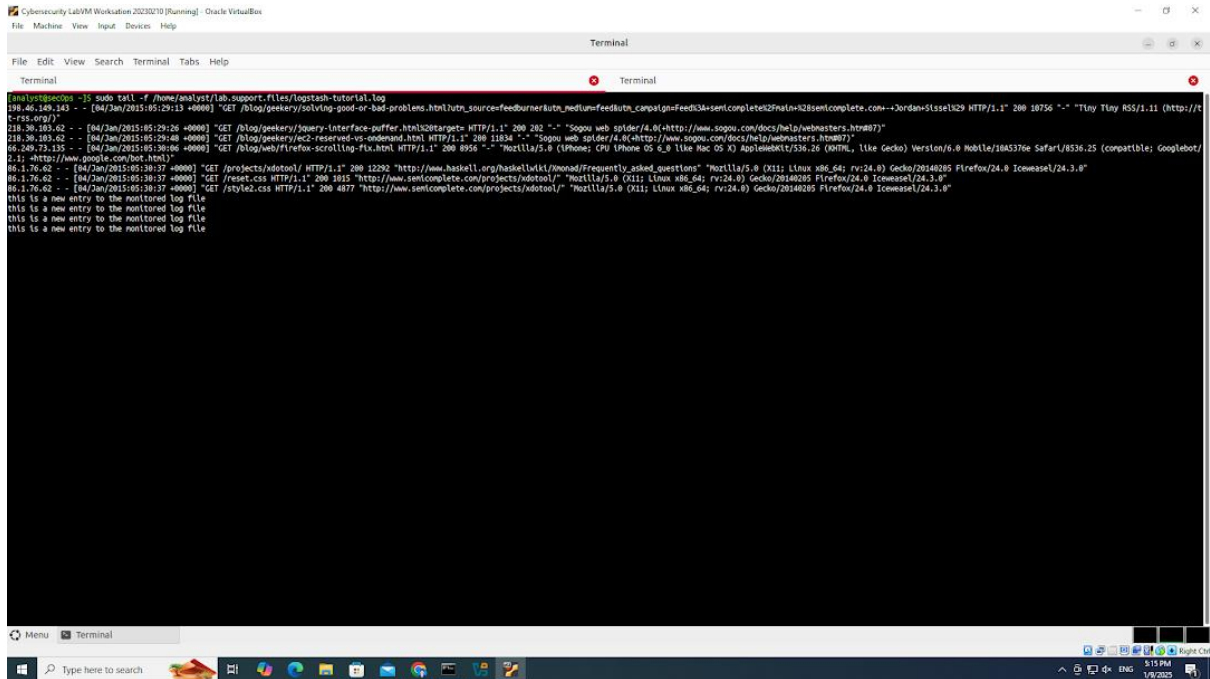
ทำการ tail ค้างไว้

แล้วลองประกาศอะไรสักอย่างใส่ไฟล์

```

[analyst@secOps ~]$ echo "this is a new entry to the monitored log file" >> lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$

```

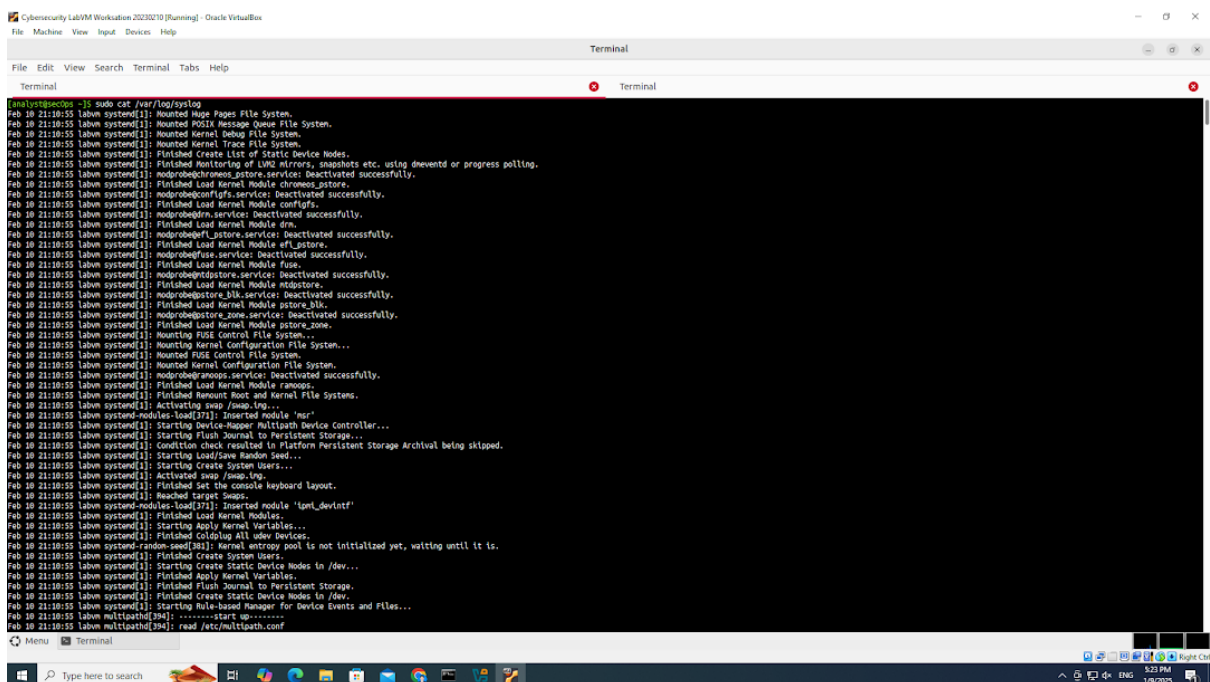



```

[analyst@secops ~]$ sudo tail -f /home/analyst/lab.support.files/logstash-tutorial.log
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain%28semicomplete.com%3A+Jordan%5B%5C%29 HTTP/1.1" 200 10756 "-" "Tiny Tunny RSS/1.11 (http://t
...
[04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/query-interface-puffer.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain%28semicomplete.com%3A+Jordan%5B%5C%29 HTTP/1.1" 200 202 "-" "Sogou web spider/4.0 (http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.183.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-on-demand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0 (http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:00 +0000] "GET /blog/web/firefox-scrolling-fits.html HTTP/1.1" 200 8955 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X; AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/vdotool/ HTTP/1.1" 200 12292 "http://www.hacktil.org/hacktilwiki/movad/frequently_asked_questions/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 IcoWeasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 3913 "http://www.semicomplete.com/projects/vdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 IcoWeasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/vdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 IcoWeasel/24.3.0"
this is a new entry to the monitored log file
this is a new entry to the monitored log file
this is a new entry to the monitored log file
this is a new entry to the monitored log file

```

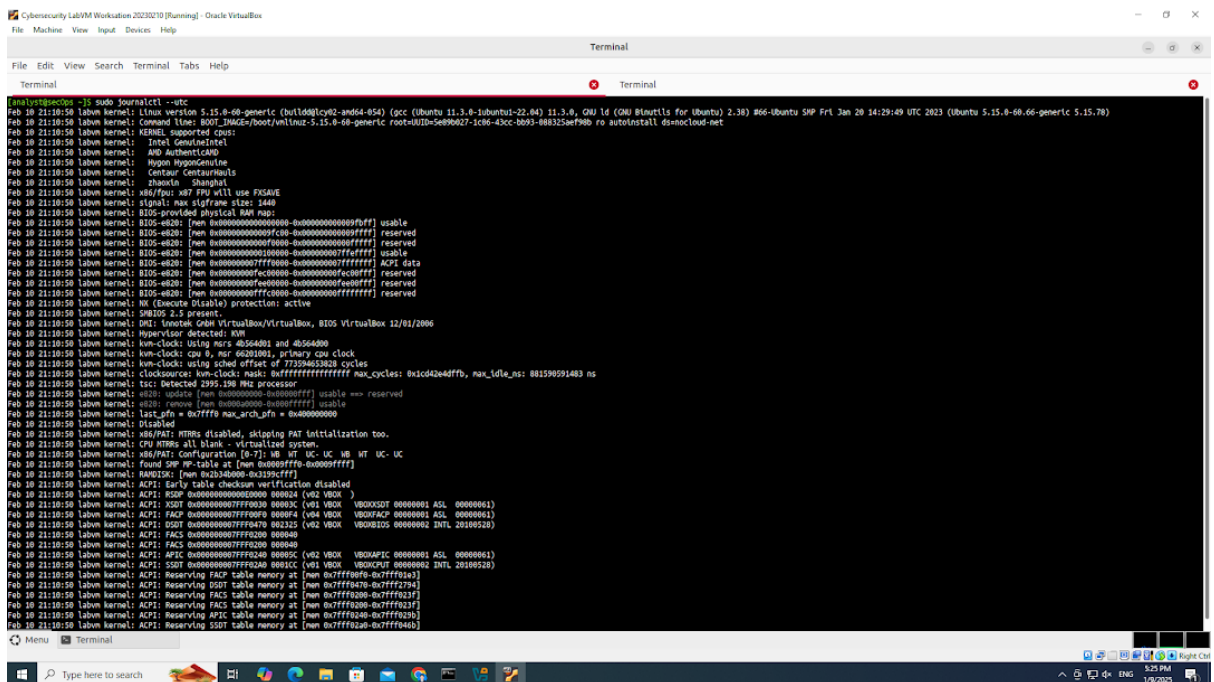
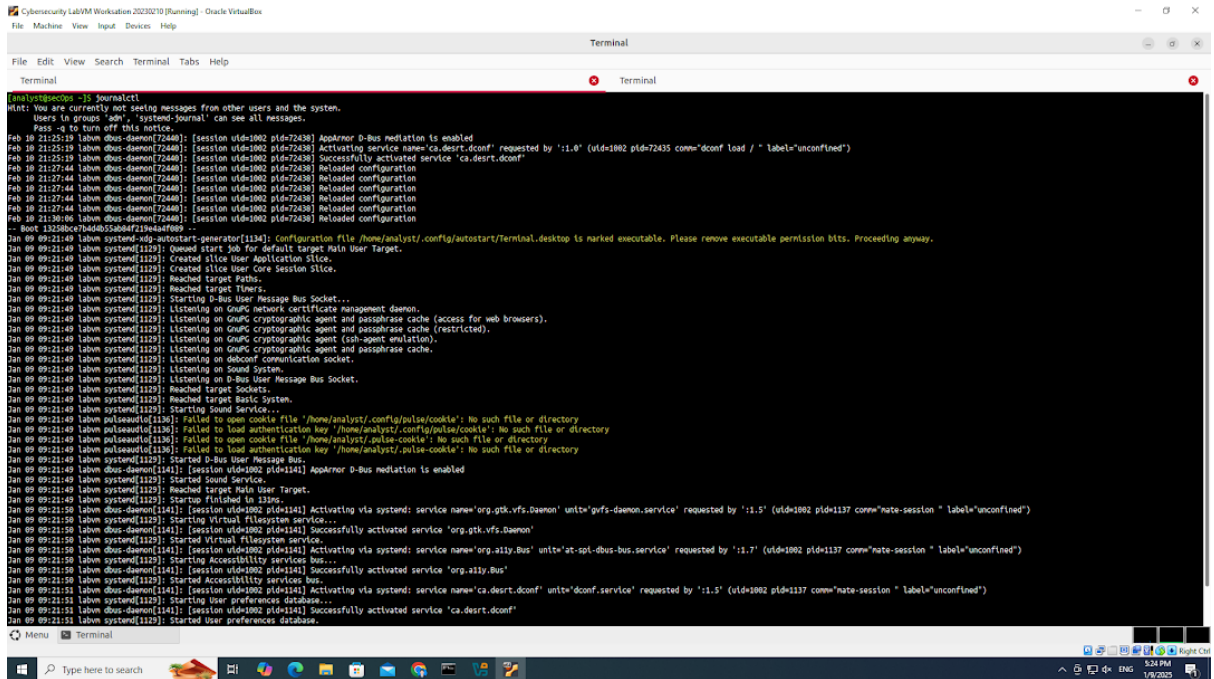
เมื่อกลับมาหน้า tail คำว่า \ไ้ก็จะพบข้อความที่ถูกประกาศ



```

[analyst@secops ~]$ sudo cat /var/log/syslog
Feb 10 21:10:55 labvm systemd[1]: Mounted Huge Pages File System.
Feb 10 21:10:55 labvm systemd[1]: Mounted POSIX Message Queue File System.
Feb 10 21:10:55 labvm systemd[1]: Mounted Kernel Debug File System.
Feb 10 21:10:55 labvm systemd[1]: Mounted Kernel Trace File System.
Feb 10 21:10:55 labvm systemd[1]: Finished Create List of Static Device Nodes.
Feb 10 21:10:55 labvm systemd[1]: Finished Monitoring of LVM2 mirrors, snapshots etc. using dmccvtd or progress polling.
Feb 10 21:10:55 labvm systemd[1]: modprobe@chromos_pstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module chromos_pstore.
Feb 10 21:10:55 labvm systemd[1]: modprobe@configfs.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module configfs.
Feb 10 21:10:55 labvm systemd[1]: modprobe@drm.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module drm.
Feb 10 21:10:55 labvm systemd[1]: modprobe@efl_pstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module efl_pstore.
Feb 10 21:10:55 labvm systemd[1]: modprobe@fuse.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module fuse.
Feb 10 21:10:55 labvm systemd[1]: modprobe@hwdmstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module hwdmstore.
Feb 10 21:10:55 labvm systemd[1]: modprobe@hwdmstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module hwdmstore.
Feb 10 21:10:55 labvm systemd[1]: modprobe@hwdmstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module hwdmstore.
Feb 10 21:10:55 labvm systemd[1]: modprobe@hwdmstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module hwdmstore.
Feb 10 21:10:55 labvm systemd[1]: modprobe@hwdmstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module hwdmstore.
Feb 10 21:10:55 labvm systemd[1]: Mounting Kernel Configuration File System...
Feb 10 21:10:55 labvm systemd[1]: Mounted Kernel Configuration File System.
Feb 10 21:10:55 labvm systemd[1]: modprobe@hwdmstore.service: Deactivated successfully.
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Module hwdmstore.
Feb 10 21:10:55 labvm systemd[1]: Finished Remount Root and Kernel File Systems.
Feb 10 21:10:55 labvm systemd[1]: Activating swap /swap.img...
Feb 10 21:10:55 labvm systemd-modules-load[371]: Inserted module 'nfs'
Feb 10 21:10:55 labvm systemd[1]: Starting Device-Mapper Multipath Device Controller...
Feb 10 21:10:55 labvm systemd[1]: Starting Flush Journal to Persistent Storage...
Feb 10 21:10:55 labvm systemd[1]: Condition check resulted in Platform Persistent Storage Archival being skipped.
Feb 10 21:10:55 labvm systemd[1]: Starting Load/Save Random Seed...
Feb 10 21:10:55 labvm systemd[1]: Starting Create System Users...
Feb 10 21:10:55 labvm systemd[1]: Activated swap /swap.img...
Feb 10 21:10:55 labvm systemd[1]: Finished Set the console keyboard layout.
Feb 10 21:10:55 labvm systemd[1]: Reached target Slices.
Feb 10 21:10:55 labvm systemd-modules-load[371]: Inserted module 'lvm_devinit'
Feb 10 21:10:55 labvm systemd[1]: Finished Load Kernel Modules.
Feb 10 21:10:55 labvm systemd[1]: Starting Apply Kernel Variables...
Feb 10 21:10:55 labvm systemd[1]: Finished Coldplug All udev Devices.
Feb 10 21:10:55 labvm systemd[1]: Kernel entropy pool is not initialized yet, waiting until it is.
Feb 10 21:10:55 labvm systemd[1]: Finished Create System Users.
Feb 10 21:10:55 labvm systemd[1]: Starting Create Static Device Nodes in /dev...
Feb 10 21:10:55 labvm systemd[1]: Finished Apply Kernel Variables.
Feb 10 21:10:55 labvm systemd[1]: Finished Flush Journal to Persistent Storage.
Feb 10 21:10:55 labvm systemd[1]: Finished Create Static Device Nodes in /dev.
Feb 10 21:10:55 labvm systemd[1]: Starting Rule-based Manager for Device Events and Files...
Feb 10 21:10:55 labvm multipathd[394]: -----start up-----
Feb 10 21:10:55 labvm multipathd[394]: read /etc/multipath.conf

```



```

Cybersecurity Lab VM Workstation 20230210 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
File Edit View Search Terminal Tabs Help

Terminal
[analyst@secops ~]$ sudo journalctl -b
Jan 09 17:05:08 labvm kernel: Linux version 5.15.0-68-generic (build@lgcy02-amd64-054) (gcc (Ubuntu 11.3.0-6ubuntu1-22.04) 11.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #66-Ubuntu SMP Fri Jan 20 14:29:49 UTC 2023 (Ubuntu 5.15.0-68-generic 5.15.78)
Jan 09 17:05:08 labvm kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-68-generic root=UUID=5e89027-1c06-43cc-b093-088325e9790b ro quiet splash zswap.enabled=1
Jan 09 17:05:08 labvm kernel: KERNEL supported cpus:
Jan 09 17:05:08 labvm kernel: Intel GenuineIntel
Jan 09 17:05:08 labvm kernel: AMD AuthenticAMD
Jan 09 17:05:08 labvm kernel: HYGON Genuine
Jan 09 17:05:08 labvm kernel: Centaur CentaurHauls
Jan 09 17:05:08 labvm kernel: shanxin Shanxin
Jan 09 17:05:08 labvm kernel: x86/fpu: Supporting xSAVE feature 0x001: 'x87 floating point registers'
Jan 09 17:05:08 labvm kernel: x86/fpu: Supporting xSAVE feature 0x002: 'SSE registers'
Jan 09 17:05:08 labvm kernel: x86/fpu: Supporting xSAVE feature 0x004: 'AVX registers'
Jan 09 17:05:08 labvm kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Jan 09 17:05:08 labvm kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Jan 09 17:05:08 labvm kernel: signal: max sigframe size: 1776
Jan 09 17:05:08 labvm kernel: BIOS-provided physical RAM map:
Jan 09 17:05:08 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009f000] usable
Jan 09 17:05:08 labvm kernel: BIOS-e820: [mem 0x000000000009f000-0x0000000000000000] reserved
Jan 09 17:05:08 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] usable
Jan 09 17:05:08 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] ACPI data
Jan 09 17:05:08 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] reserved
Jan 09 17:05:08 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] reserved
Jan 09 17:05:08 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] reserved
Jan 09 17:05:08 labvm kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000] usable
Jan 09 17:05:08 labvm kernel: NX (Execute Disable) protection: active
Jan 09 17:05:08 labvm kernel: DR100 2.0 present.
Jan 09 17:05:08 labvm kernel: DMI: Innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Jan 09 17:05:08 labvm kernel: Hypervisor detected: KVM
Jan 09 17:05:08 labvm kernel: kvm-clock: Using msrc 0x564d01 and 0x564d00
Jan 09 17:05:08 labvm kernel: kvm-clock: cpu 0, msr 18001001, primary cpu clock
Jan 09 17:05:08 labvm kernel: kvm-clock: using sched offset of 487909995 cycles
Jan 09 17:05:08 labvm kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idt_ns: 881398391483 ns
Jan 09 17:05:08 labvm kernel: tsc: Detected 3600.002 MHz processor
Jan 09 17:05:08 labvm kernel: smp: update (mem 0x00000000-0x00000000) usable *** reserved
Jan 09 17:05:08 labvm kernel: smp: remove (mem 0x00000000-0x00000000) usable
Jan 09 17:05:08 labvm kernel: last_pfn = 0x120000 max_arch_pfn = 0x000000000
Jan 09 17:05:08 labvm kernel: x86/PMU: Configuration (0-7): 0B 0C 0C 0C 0B 0F 0C 0F
Jan 09 17:05:08 labvm kernel: total RAM covered: 4096M
Jan 09 17:05:08 labvm kernel: Found optimal setting for nrttr clean up
Jan 09 17:05:08 labvm kernel: prn_size: 64K, chunk_size: 1K, max_rag: 3, lose cover RAM: 0C
Jan 09 17:05:08 labvm kernel: smp: update (mem 0x00000000-0xffffffff) usable *** reserved
Jan 09 17:05:08 labvm kernel: last_pfn = 0x120000 max_arch_pfn = 0x000000000
Jan 09 17:05:08 labvm kernel: found SMP MP-table at [mem 0x00000000-0x00000000]
Jan 09 17:05:08 labvm kernel: RAM010K: (mem 0x3667000-0x3667000)
Jan 09 17:05:08 labvm kernel: ACPI: Early table checksum verification disabled
Jan 09 17:05:08 labvm kernel: ACPI: RSDP 0x0000000000000000 000024 (v02 VBOX )
Jan 09 17:05:08 labvm kernel: ACPI: XSDT 0x0000000000000000 00003C (v01 VBOX VBOXXSDT 00000001 ASL 00000001)
Jan 09 17:05:08 labvm kernel: ACPI: FACP 0x0000000000000000 000074 (v04 VBOX VBOXFACP 00000001 ASL 00000001)
Jan 09 17:05:08 labvm kernel: ACPI: DSDT 0x0000000000000000 001233 (v02 VBOX VBOXDSDT 00000002 INTL 20100518)
Jan 09 17:05:08 labvm kernel: ACPI: FACS 0x0000000000000000 000040
Jan 09 17:05:08 labvm kernel: ACPI: FACS 0x0000000000000000 000040
Jan 09 17:05:08 labvm kernel: ACPI: APIC 0x0000000000000000 00005C (v02 VBOX VBOXAPIC 00000001 ASL 00000001)

```

```

Cybersecurity Lab VM Workstation 20230210 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
File Edit View Search Terminal Tabs Help

Terminal
[analyst@secops ~]$ sudo journalctl -u nginx.service --since today
-- No entries --
[analyst@secops ~]$

```

```

CyberSecurity Lab VM Workstation 20230210 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
File Edit View Search Terminal Tabs Help

Terminal
[linux@ubuntu:~]$ sudo journalctl -k
Jan 20 17:05:08 labvm kernel: Linux version 5.15.0-68-generic (build@lgcy02-and64-854) (gcc (Ubuntu 11.3.0-6ubuntu1-22.44) 11.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #66-Ubuntu SMP Fri Jan 20 14:29:49 UTC 2023 (Ubuntu 5.15.0-68-generic 5.15.78)
Jan 20 17:05:08 labvm kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-68-generic root=UUID=5e9b0627-1c06-43cc-b093-888325ae79b0 ro quiet splash zswap.enabled=1
Jan 20 17:05:08 labvm kernel: KASLR supported Gpus:
Jan 20 17:05:08 labvm kernel: Intel GenuineIntel
Jan 20 17:05:08 labvm kernel: AMD AuthenticAMD
Jan 20 17:05:08 labvm kernel: Hypo: HypoGenuine
Jan 20 17:05:08 labvm kernel: Centaur CentaurHauls
Jan 20 17:05:08 labvm kernel: Shantui Shantui
Jan 20 17:05:08 labvm kernel: x86/fpu: Supporting XSAVES feature 0x001: 'x87 floating point registers'
Jan 20 17:05:08 labvm kernel: x86/fpu: Supporting XSAVES feature 0x002: 'SSE registers'
Jan 20 17:05:08 labvm kernel: x86/fpu: Supporting XSAVES feature 0x004: 'XMM registers'
Jan 20 17:05:08 labvm kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Jan 20 17:05:08 labvm kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Jan 20 17:05:08 labvm kernel: smpol: max smpcra size: 376
Jan 20 17:05:08 labvm kernel: BIOS-provided physical RAM map:
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] usable
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] reserved
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] reserved
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] usable
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] ACPI data
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] reserved
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] reserved
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] reserved
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] reserved
Jan 20 17:05:08 labvm kernel: BIOS-e820: [mem 0x00000000-0x00000000] usable
Jan 20 17:05:08 labvm kernel: NX (Execute Disable) protection: active
Jan 20 17:05:08 labvm kernel: SMBIOS 2.5 present.
Jan 20 17:05:08 labvm kernel: DR1: Intel® Core™ VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Jan 20 17:05:08 labvm kernel: Hypervisor detected: KVM
Jan 20 17:05:08 labvm kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Jan 20 17:05:08 labvm kernel: kvm-clock: csn 6, msrc 1b020101, primary cse clock
Jan 20 17:05:08 labvm kernel: kvm-clock: using sched offset of 407869995 cycles
Jan 20 17:05:08 labvm kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dfff, max_tdn: 0x1390591483 ns
Jan 20 17:05:08 labvm kernel: tsc: Detected 3600.000 MHz processor
Jan 20 17:05:08 labvm kernel: e820: update [mem 0x00000000-0x00000000] usable ==> reserved
Jan 20 17:05:08 labvm kernel: e820: remove [mem 0x00000000-0x00000000] usable
Jan 20 17:05:08 labvm kernel: last_pfn = 0x1200000 max_arch_pfn = 0x00000000
Jan 20 17:05:08 labvm kernel: x86/PAT: Configuration [0-7]: WB UC UC- UC- WB UC- WT
Jan 20 17:05:08 labvm kernel: total RAM covered: 4096
Jan 20 17:05:08 labvm kernel: gran_size: 0x10 chunk_size: 10 num_nops: 3 lose cover RAM: 0x0
Jan 20 17:05:08 labvm kernel: e820: update [mem 0x00000000-0x00000000] usable ==> reserved
Jan 20 17:05:08 labvm kernel: last_pfn = 0x1200000 max_arch_pfn = 0x00000000
Jan 20 17:05:08 labvm kernel: found SMP MP-table at [mem 0x00000000-0x00000000]
Jan 20 17:05:08 labvm kernel: RAMDISK: (mem 0x386f7000-0x386f7fff)
Jan 20 17:05:08 labvm kernel: ACPI: Early table checksum verification disabled
Jan 20 17:05:08 labvm kernel: ACPI: SDT 0x0000000000000000 00000000 (v0 VBOX VBOXSDT 00000001 ASL 00000001)
Jan 20 17:05:08 labvm kernel: ACPI: XSDT 0x0000000000000000 00000000 (v0 VBOX VBOXXSDT 00000001 ASL 00000001)
Jan 20 17:05:08 labvm kernel: ACPI: FACS 0x0000000000000000 00000000 (v0 VBOX VBOXFACS 00000001 ASL 00000001)
Jan 20 17:05:08 labvm kernel: ACPI: DSDT 0x0000000000000000 00000000 (v0 VBOX VBOXDSDT 00000001 ASL 00000001)
Jan 20 17:05:08 labvm kernel: ACPI: FACS 0x0000000000000000 00000000 (v0 VBOX VBOXFACS 00000001 ASL 00000001)
Jan 20 17:05:08 labvm kernel: ACPI: APIC 0x0000000000000000 00000000 (v0 VBOX VBOXAPIC 00000001 ASL 00000001)

```

```

CyberSecurity Lab VM Workstation 20230210 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
File Edit View Search Terminal Tabs Help

Terminal
[linux@ubuntu:~]$ sudo journalctl -f
Jan 20 17:05:14 labvm systemd[526]: Started Disk Manager.
Jan 20 17:05:14 labvm systemd[526]: Acquired the name org.freedesktop.UDisks2 on the system message bus
Jan 20 17:05:15 labvm kernel: 17:05:15.007219 main vboxService 7.0.6 /155176 (verbosity: 0) Linux-and04 (Jan 11 2023 15:34:33) release log
Jan 20 17:05:15 labvm kernel: 17:05:15.007223 main Log opened 2023-01-10T17:05:15.00722996Z
Jan 20 17:05:15 labvm kernel: 17:05:15.007374 main OS Product: Linux
Jan 20 17:05:15 labvm kernel: 17:05:15.007431 main OS Release: 5.15.0-68-generic
Jan 20 17:05:15 labvm kernel: 17:05:15.007477 main OS Version: mac-ubuntu SMP Fri Jan 20 14:29:49 UTC 2023
Jan 20 17:05:15 labvm kernel: 17:05:15.007521 main Executable: /opt/VBoxGuestAdditions-7.0.6/bin/VBoxService
Jan 20 17:05:15 labvm kernel: 17:05:15.007522 main Process ID: 700
Jan 20 17:05:15 labvm kernel: 17:05:15.007523 main Package type: LINUX_64BITS_GENERIC
Jan 20 17:05:15 labvm kernel: 17:05:15.008089 main 7.0.6 /155176 started, Verbose level = 0
Jan 20 17:05:15 labvm kernel: 17:05:15.022738 main VBoxGuestCtrlDetectPeakGuestCancelSupport: Supported (81)
Jan 20 17:05:15 labvm kernel: 17:05:15.022738 main VBoxGuestCtrlDetectPeakGuestCancelSupport: Supported (81)
Jan 20 18:05:16 labvm systemd[1]: Started vboxadd-service.service.
Jan 20 18:05:16 labvm systemd[1]: VirtualBox Guest Addition service started.
Jan 20 18:05:16 labvm systemd[1]: networkd-dispatcher[511]: No valid path found for fw
Jan 20 18:05:16 labvm systemd-resolve[394]: Clock change detected. Flushing caches.
Jan 20 18:05:16 labvm systemd[1]: networkd-dispatcher[511]: Deactivated successfully.
Jan 20 18:05:16 labvm systemd[1]: Finished OpenvSwitch configuration for cleanup.
Jan 20 18:05:16 labvm systemd[1]: Started Dispatcher daemon for systemd-networkd.
Jan 20 18:05:16 labvm kernel: openvswitch: Open vswitch switching datapath
Jan 20 18:05:16 labvm ovs-ctl[638]: * Inserting openvswitch module
Jan 20 18:05:16 labvm ovs-ctl[620]: * Starting ovs-vswitchd
Jan 20 18:05:16 labvm ovs-ctl[635]: * Enabling remote OVSDB managers
Jan 20 18:05:16 labvm systemd[1]: Started Open vSwitch Forwarding Unit.
Jan 20 18:05:16 labvm systemd[1]: Starting Open vswitch...
Jan 20 18:05:16 labvm systemd[1]: Finished Open vswitch.
Jan 20 18:05:16 labvm systemd[1]: Reached Target Network.
Jan 20 18:05:16 labvm systemd[1]: Reached target Network is online.
Jan 20 18:05:16 labvm systemd[1]: Started download data for packages that failed at package install time.
Jan 20 18:05:16 labvm systemd[1]: Started check to see whether there is a new version of Ubuntu available.
Jan 20 18:05:16 labvm systemd[1]: Reached Target Time Units.
Jan 20 18:05:16 labvm systemd[1]: Starting Network Time Service...
Jan 20 18:05:16 labvm systemd[1]: Starting Open vswitch Record Hostname...
Jan 20 18:05:16 labvm systemd[1]: Condition check resulted in Pollinate to seed the pseudo random number generator being skipped.
Jan 20 18:05:16 labvm systemd[1]: Starting /etc/rc-local Compatibility...
Jan 20 18:05:16 labvm systemd[1]: Starting OpenSSH Server daemon...
Jan 20 18:05:16 labvm systemd[1]: Starting Permit User Sessions...
Jan 20 18:05:16 labvm systemd[1]: Condition check resulted in Ubuntu Pro Background Auto Attach being skipped.
Jan 20 18:05:16 labvm systemd[1]: Starting xfsd FIF server...
Jan 20 18:05:16 labvm systemd[1]: Starting LSB: Starts or stops the xinetd daemon...
Jan 20 18:05:16 labvm systemd[1]: Started xfsd FIF server.
Jan 20 18:05:16 labvm systemd[1]: Finished Permit User Sessions.
Jan 20 18:05:16 labvm systemd[1]: Starting Light Display Manager...
Jan 20 18:05:16 labvm ovs-ctl[638]: ovs-vswitchd[638]: ovs-vswitchd - no-wait add OpenvSwitch . external-ids hostname=labvm
Jan 20 18:05:16 labvm systemd[1]: Finished Open vswitch Record Hostname.
Jan 20 18:05:16 labvm systemd[1]: Reloading.
Jan 20 18:05:17 labvm ntpd[638]: ntpd 4.2.0-35.13728-o Wed Feb 16 17:13:02 UTC 2022 (1): Starting
Jan 20 18:05:17 labvm ntpd[638]: Command line: /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 117:127
Jan 20 18:05:17 labvm ntpd[638]: .....
Jan 20 18:05:17 labvm ntpd[638]: ntpd-4 is maintained by Network Time Foundation
Jan 20 18:05:17 labvm ntpd[638]: Inc. (NTP), a non-profit 501(c)(3) public-benefit
Jan 20 18:05:17 labvm ntpd[638]: corporation. Support and training for ntp-4 are

```