**Technical Operations (TechOps)**

OS Admin

Linux Narrative Exercises

© FDM Group Ltd 2011. All Rights Reserved.

Any unauthorised reproduction or distribution in part  
or in whole will constitute an infringement of copyright.

|  |
| --- |
| Page left intentionally blank |

# Logfile Questions

### Inspecting the logging of login attempts.

As root, run the command

touch /etc/now

This updates the modification time of /etc/now.

Now run the command ‘find /var/log –type f –newer /etc/now’ . This will find all the files under /var/log which have been modified more recently than /etc/now. There should not be any or just a few if you are unlucky

/var/log/cron

/var/log/messages

Note ‘art’ is a non-existent user. **Attempt to login to your VM as the user ‘art’. Hit ‘return’ just one time on seeing the prompt for a password**. Then try after pressing ‘return’ enough times to be kicked out.

Now, run command ‘find /var/log –type f –newer /etc/now’ again. Which files have been modified? These should show up in the list.

/var/log/audit/audit.log

/var/log/secure

/var/log/btmp

These have been updated as a result of the failed login attempt.

Run ‘tail /var/log/audit/audit.log | grep USER’ Look at the USER\_A six sync UTH messages.

Can you identify the IP address associated with the failed login attempt?

Can you tell which account they were trying to login as? (No!)

What does it say about the account? (unknown)

What parameter tells you you were using the secure shell protocol? (exe/terminal)

type=USER\_LOGIN msg=audit(1658232761.808:2274): pid=4538 uid=0 auid=4294967295 ses=4294967295 subj=system\_u:system\_r:sshd\_t:s0-s0:c0.c1023 msg='op=login acct="(unknown)" exe="/usr/sbin/sshd" hostname=? addr=86.134.136.135 terminal=ssh res=failed' (NB: have to keep pressing enter until it kicks you out)

type=USER\_AUTH msg=audit(1658232761.205:2266): pid=4538 uid=0 auid=4294967295 ses=4294967295 subj=system\_u:system\_r:sshd\_t:s0-s0:c0.c1023 msg='op=password acct="(unknown)" exe="/usr/sbin/sshd" hostname=? addr=86.134.136.135 terminal=ssh res=failed'

The IP address of the originator can be seen in the record. One of the USER\_AUTH records has the hostname= and addr= parameters. The account name (acct=) is ‘unknown’. So the only thing you can say from this record is that they were trying to login to an undefined user account. The terminal=ssh parameter shows the login attempt used secure shell.

What extra information of significance does /var/log/secure give you?

Jul 19 12:50:02 ml-refvm-422293 sshd[5066]: pam\_unix(sshd:session): session opened for user instructor by (uid=0)

Jul 19 12:50:25 ml-refvm-422293 sudo: instructor : TTY=pts/1 ; PWD=/home/instructor ; USER=root ; COMMAND=/bin/bash

Jul 19 12:50:25 ml-refvm-422293 sudo: pam\_unix(sudo-i:session): session opened for user root by instructor(uid=0)

Jul 19 12:50:52 ml-refvm-422293 sshd[5060]: Failed password for invalid user art from 86.134.136.135 port 49340 ssh2

Jul 19 12:55:03 ml-refvm-422293 sshd[5229]: Invalid user art from 86.134.136.135 port 49535

Jul 19 12:55:03 ml-refvm-422293 sshd[5229]: input\_userauth\_request: invalid user art [preauth]

Jul 19 12:55:04 ml-refvm-422293 sshd[5229]: Failed none for invalid user art from 86.134.136.135 port 49535 ssh2

Jul 19 12:55:04 ml-refvm-422293 sshd[5229]: Failed password for invalid user art from 86.134.136.135 port 49535 ssh2

Jul 19 12:55:04 ml-refvm-422293 sshd[5229]: Failed password for invalid user art from 86.134.136.135 port 49535 ssh2

Jul 19 12:55:04 ml-refvm-422293 sshd[5229]: Connection closed by 86.134.136.135 port 49535 [preauth]

It shows that the login attempt was to an invalid user called ‘art’. (This username was not in the audit.log) The fact that the user might think there is an account called ‘art’ might be helpful in resolving the problem.

Do not attempt to look at /var/log/btmp, it is binary data. Run ‘lastb | head’ What does this show you?

[root@ml-refvm-422293 ~]# lastb | head

art ssh:notty host86-134-136-1 Tue Jul 19 12:55 - 12:55 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 12:55 - 12:55 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 12:50 - 12:50 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 12:49 - 12:49 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 12:12 - 12:12 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 12:12 - 12:12 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 12:09 - 12:09 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 12:08 - 12:08 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 11:49 - 11:49 (00:00)

art ssh:notty host86-134-136-1 Tue Jul 19 11:49 - 11:49 (00:00)

The output shows details of the last ten bad login attempts. It shows the account name (valid or invalid) associated with the attempts, the time and the hostname/IP of the originating machine. No real extra information but a nice short display.

Repeat the above login attempt but use the sync account name rather than ‘art’. Do not actually login. (Hit return when asked for a password.) What is different?

type=**USER**\_AUTH msg=audit(1658240046.978:3715): pid=6386 uid=0 auid=4294967295 ses=4294967295 subj=system\_u:system\_r:sshd\_t:s0-s0:c0.c1023 msg='op=password acct="instructor" exe="/usr/sbin/sshd" hostname=? addr=86.134.136.135 terminal=ssh res=failed'

type=**USER**\_AUTH msg=audit(1658240170.002:3766): pid=6426 uid=0 auid=4294967295 ses=4294967295 subj=system\_u:system\_r:sshd\_t:s0-s0:c0.c1023 msg='op=password acct="sync" exe="/usr/sbin/sshd" hostname=? addr=86.134.136.135 terminal=ssh res=failed'

The audit.log file ‘acct=’ parameter is no longer set to ‘unknown’ but mentions ‘sync’. The secure file is not updated after just one password attempt. Its is updated after two attempts. In /var/log/secure, instead of

Invalid user art from 90.255.187.20 port 61099

input\_userauth\_request: invalid user art [preauth]

Failed none for invalid user art from 90.255.187.20 port 61099 ssh2

You get

Failed password for sync from 90.255.187.20 port 61179 ssh2

The lastb command output is similar for both examples.

### Controlling logging behavior.

We pretty much have all the detail we might wish for in the logs we have seen, maybe too much? It might be that we would like a more summarized view of authentication events, whilst keeping the full detail in case we need it.

Edit /etc/rsyslog.conf and change:

authpriv.\* /var/log/secure

to

authpriv.\* /var/log/secure

authpriv.error /var/log/authpriv.error

The extra line sends messages from the authpriv facility which are classified as having a priority error or above to /var/log/authpriv.error.

Once you have made the change, run a command to restart the rsyslog service.

systemctl restart rsyslog

Run the commands

logger –p authpriv.error “Test 1”

logger –p authpriv.warn “Another message”

Which appears in /var/log/authpriv.error and which in /var/log/secure?

“Test 1” appears in both files.

“Another message” appears only in in /var/log/secure.

Set up two putty sessions (sudo to root) and arrange each screen so that you have the two side by side in the top two-thirds of the window. In one widow run ‘tail –f /var/log/secure’ and in the other ‘tail –f /var/log/authpriv.error’. Note: The ‘tail –f’ command follows a file’s growth, displaying it to the screen.

Now in a third putty session:

Attempt (and fail) to login as instructor. Then do this again using fictitious username ‘lego’.

What is the difference in messages logged to the two files?

[root@ml-refvm-422293 etc]# tail -f /var/log/secure

Jul 19 14:14:06 ml-refvm-422293 sshd[6386]: Failed password for instructor from 86.134.136.135 port 49773 ssh2

Jul 19 14:14:07 ml-refvm-422293 sshd[6386]: Failed password for instructor from 86.134.136.135 port 49773 ssh2

Jul 19 14:14:07 ml-refvm-422293 sshd[6386]: Connection closed by 86.134.136.135 port 49773 [preauth]

Jul 19 14:16:10 ml-refvm-422293 sshd[6426]: Failed password for sync from 86.134.136.135 port 49822 ssh2

Jul 19 14:16:11 ml-refvm-422293 sshd[6426]: Failed password for sync from 86.134.136.135 port 49822 ssh2

Jul 19 14:16:11 ml-refvm-422293 sshd[6426]: Connection closed by 86.134.136.135 port 49822 [preauth]

Jul 19 14:28:34 ml-refvm-422293 polkitd[783]: Registered Authentication Agent for unix-process:6558:1950946 (system bus name :1.1023 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en\_GB.UTF-8)

Jul 19 14:28:34 ml-refvm-422293 polkitd[783]: Unregistered Authentication Agent for unix-process:6558:1950946 (system bus name :1.1023, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en\_GB.UTF-8) (disconnected from bus)

Jul 19 14:30:49 ml-refvm-422293 instructor: Test 1

Jul 19 14:31:11 ml-refvm-422293 instructor: Another message

Jul 19 14:34:28 ml-refvm-422293 sshd[6647]: Accepted password for instructor from 86.134.136.135 port 50311 ssh2

Jul 19 14:34:29 ml-refvm-422293 sshd[6647]: pam\_unix(sshd:session): session opened for user instructor by (uid=0)

Jul 19 14:35:11 ml-refvm-422293 sudo: instructor : TTY=pts/1 ; PWD=/home/instructor ; USER=root ; COMMAND=/bin/bash

Jul 19 14:35:11 ml-refvm-422293 sudo: pam\_unix(sudo-i:session): session opened for user root by instructor(uid=0)

Jul 19 14:39:41 ml-refvm-422293 sshd[6788]: Failed password for instructor from 86.134.136.135 port 50438 ssh2

Jul 19 14:39:41 ml-refvm-422293 sshd[6788]: Failed password for instructor from 86.134.136.135 port 50438 ssh2

Jul 19 14:39:41 ml-refvm-422293 sshd[6788]: Connection closed by 86.134.136.135 port 50438 [preauth]

Jul 19 14:40:05 ml-refvm-422293 sshd[6813]: Invalid user lego from 86.134.136.135 port 50458

Jul 19 14:40:05 ml-refvm-422293 sshd[6813]: input\_userauth\_request: invalid user lego [preauth]

Jul 19 14:40:06 ml-refvm-422293 sshd[6813]: Failed none for invalid user lego from 86.134.136.135 port 50458 ssh2

Jul 19 14:40:06 ml-refvm-422293 sshd[6813]: Failed password for invalid user lego from 86.134.136.135 port 50458 ssh2

Jul 19 14:40:06 ml-refvm-422293 sshd[6813]: Failed password for invalid user lego from 86.134.136.135 port 50458 ssh2

Jul 19 14:40:07 ml-refvm-422293 sshd[6813]: Connection closed by 86.134.136.135 port 50458 [preauth]

No messages appear in authpriv.error. The usual messages appear in /var/log/secure.

It will say invalid user for loge but not for instructor. It also shows us the loggins in real time.

Is there any advantage to having the authpriv.error log?

It is arguable that authpriv.error provides enough information for the system administrator to know what is going on.

### Boot messages

System boot messages are often a good source of information because sometimes applications/system services fail ‘from the get-go’! Knowing that they have not worked at all since boot can help when troubleshooting. For example, it is less likely to be a use error and more likely to be a configuration error. The standard unix command used to show unix boot messages is ‘dmesg’. How many lines of boot information does dmesg show?

dmesg | wc –l

1377 – but this will vary

The ‘new’ systemd, the daemon which initializes the system came in as default with Centos 7.14. It writes boot messages to its own buffer or message log.

Display all the messages from the current boot.

journalctl –b

#### Enable persistent boot message logging.

In file /etc/systemd/journald.conf:

Uncomment line Storage

Set the option to persistent