

Blogs

Told you, we love sharing!

[Home \(/\)](#) / [Blog \(http://www.tothenew.com/blog/\)](http://www.tothenew.com/blog/) / [Technology \(http://www.tothenew.com/blog/category/technology/\)](http://www.tothenew.com/blog/category/technology/) / [AWS \(http://www.tothenew.com/blog/category/technology/aws-2/\)](http://www.tothenew.com/blog/category/technology/aws-2/)

Category

Subscribe to Our Blog

Auditing Your Ubuntu Servers

AWS ([HTTP://WWW.TOTHENEW.COM/BLOG/CATEGORY/TECHNOLOGY/AWS-2/](http://www.tothenew.com/blog/category/technology/aws-2/))

23 / MAR / 2015 BY [RANVIJAY JAMWAL \(HTTP://WWW.TOTHENEW.COM/BLOG/AUTHOR/RANVIJAYINTELLIGRAPE-COM/\)](http://www.tothenew.com/blog/author/ranvijayintelligrape-com/)
([HTTP://WWW.TOTHENEW.COM/BLOG/AUDITING-YOUR-UBUNTU-SERVERS/#RESPOND](http://www.tothenew.com/blog/auditing-your-ubuntu-servers/#RESPOND))

[0 COMMENTS](#)

Share this blog

Email

Twitter

Facebook

LinkedIn

Google+

You might be wondering how to audit your Ubuntu server / your Ubuntu local machine. Well, In this blog I will show you how easy it is do so. Auditing can be done by many ways of which few we shall discuss here. There are 3 following scenarios which we will be discussing :-

1.Finding from where logins are done & commands are executed

We can find the IP from where a ssh login has been done and commands have been executed. Also we can get the status of logins & those commands.

Suppose a Server has 2 users :-

1. Ubuntu which has sudo access.
 2. ranvijay is a another user created by useradd.
- (password login to server has been enabled)

Login to your server using Ubuntu user.

Also, login to server in with user ranvijay from another machine which might be running on the same or other network.

Now, if we want to check from where the ssh logins have been made

Run command ->

“**pstree -p**” and grep whatever command you want to audit

like “**grep sshd**”

or simply “**ps -ef | grep sshd**”

This will return PIDs of ssh logins which have been processed till now.

Logs are stored in auth.log file

So,

"sudo grep 2448 /var/log/auth.log" (2248 is the process ID & it may vary in your server)

After running the above command, multiple PIDs will be shown, so you can filter the output according to your use.

You would get a similar output :-

```
$ pstree -p | grep watch
|      |-sshd(15243)---sshd(15342)---bash(15343)---watch(15450)
$ sudo grep 15243 /var/log/auth.log
Mar  7 15:37:29 XXXXXXXXXXX sshd[15243]: Accepted publickey for XXXXXXXXXXX from
12.34.56.78 port 48218 ssh2
Mar  7 15:37:29 XXXXXXXXXXX sshd[15243]: pam_unix(sshd:session): session opened for user
XXXXXXXXXXXX by (uid=0)
Mar  7 15:37:44 XXXXXXXXXXX sudo: XXXXXXXXXXX : TTY=pts/7 ; PWD=/home/XXXXXXXXXXXX ;
USER=root ; COMMAND=/bin/grep 15243 /var/log/auth.log
```

2.For finding who changed / executed a particular file /process /system calls

For this, we have the auditd tool

Install it by using the following command.

"apt-get install auditd audispd-plugins"

Auditd works on some user defined rules. So, now we have to set the rules.

These rules specify for which file to & the operations on the file to keep track of

Now run command ->

"vim /etc/audit/audit.rules"

Here write rules like below :-

```
# First rule - delete all
-D

# increase the buffers to survive stress events. make this bigger for busy
systems.
-b 1024

# monitor unlink() and rmdir() system calls.
-a exit,always -S unlink -S rmdir

# monitor open() system call by Linux UID 1001.
-a exit,always -S open -F loginuid=1001

# monitor write-access and change in file properties (read/write/execute) of
the following files.
-w /etc/group -p wa
-w /etc/passwd -p wa
-w /etc/shadow -p wa
-w /etc/sudoers -p wa

# monitor read-access of the following directory.
-w /etc/secret_directory -p r

# lock the audit configuration to prevent any modification of this file.
-e 2
```

Note:- When you write the line highlighted you wont be able to edit the audit.rules file again. There is an alternative to you opening the file and editing it. If you don't want to edit the file you can directly define rules via command.

"auditctl -a exit,always -F path=/etc/passwd -F perm=wa"

This will append audit.rules file & activate audit on passwd file.

A Few more auditctl commands:-

To see all system calls made by a program:

"auditctl -a entry,always -S all -F pid=1005"

To see files opened by a specific user:

"auditctl -a exit,always -S open -F auid=510"

To see unsuccessful open call's:

"auditctl -a exit,always -S open -F success!=0"

Here are a few switches :-

r = read

w = write

x = execute

a = attribute change

Restart the service.

"sudo service auditd restart"

Now, run the below command with the file you want to edit.

"ausearch -f /etc/passwd"

This will audit file passwd and return results.

```
time->Sun May 12 19:22:31 2013
type=PATH msg=audit(1368411751.734:94): item=0 name="/etc/passwd" inode=655761 dev=08:01 mode=0100644
ouid=0 ogid=0 rdev=00:00
type=CWD msg=audit(1368411751.734:94): cwd="/home/xmodulo"
type=SYSCALL msg=audit(1368411751.734:94): arch=40000003 syscall=306 success=yes exit=0 a0=ffffff9c a1
=8624900 a2=1a6 a3=8000 items=1 ppid=14971 pid=14972 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 s
gid=0 fsgid=0 tty=pts2 ses=19 comm="chmod" exe="/bin/chmod" key=(null)
```

3. Now auditing User actions (Who What ,How Much & When)

For this, we need to Install acct

"sudo apt-get install acct"

This gives many commands few of which are :-

ac : ac command prints the statistics of user logins/logouts (connect time) in hours.

ac -d : Using command "ac -d" will prints out the total login time in hours by day-wise.

ac ranvijay : To get the total login statistics time of user "ranvijay" in hours, use the command as.

sa -c : The command "sa -c" displays the highest memory percentage usage of users.

lastcomm : The “lastcomm” command is used to search and display previously executed user commands information. You can also search commands executed by individual usernames.

Run command ->

“lastcomm username”

or you can find which user ran a particular command & when

“lastcomm ls”or “lastcomm rm”

```
root@intelligrape-Lenovo-G500:/home/intelligrape# lastcomm intelligrape
lastcomm      intellig pts/4      0.00 secs Mon Mar 23 17:41
chrome        F X intellig  —      0.72 secs Mon Mar 23 16:55
chrome-sandbox      intellig  —      0.00 secs Mon Mar 23 17:40
CompositorTileW F X intellig  —      2.42 secs Mon Mar 23 17:34
CompositorTileW F X intellig  —      3.44 secs Mon Mar 23 17:33
chrome-sandbox      intellig  —      0.00 secs Mon Mar 23 17:34
chrome        F X intellig  —      1.50 secs Mon Mar 23 17:33
chrome-sandbox      intellig  —      0.00 secs Mon Mar 23 17:33
HTMLParserThrea F X intellig  —      0.12 secs Mon Mar 23 17:33
chrome-sandbox      intellig  —      0.00 secs Mon Mar 23 17:33
WorkerPool/2729 F X intellig  —      6.82 secs Mon Mar 23 17:31
chrome-sandbox      intellig  —      0.00 secs Mon Mar 23 17:33
chrome        F X intellig  —      0.81 secs Mon Mar 23 17:31
chrome-sandbox      intellig  —      0.00 secs Mon Mar 23 17:31
```

All this will really help you keep track of the users, keep your server safe & let you know who is responsible for which action.

Tag -

[Audit \(Http://Www.Tothenew.Com/Blog/Tag/Audit/\)](http://www.tothenew.com/blog/tag/audit/)

[Audit Logging \(Http://Www.Tothenew.Com/Blog/Tag/Audit-Logging/\)](http://www.tothenew.com/blog/tag/audit-logging/)

[Aws \(Http://Www.Tothenew.Com/Blog/Tag/Aws/\)](http://www.tothenew.com/blog/tag/aws/)

[Log \(Http://Www.Tothenew.Com/Blog/Tag/Log/\)](http://www.tothenew.com/blog/tag/log/)

[Server \(Http://Www.Tothenew.Com/Blog/Tag/Server/\)](http://www.tothenew.com/blog/tag/server/)

[Track User \(Http://Www.Tothenew.Com/Blog/Tag/Track-User/\)](http://www.tothenew.com/blog/tag/track-user/)

[Ubuntu \(Http://Www.Tothenew.Com/Blog/Tag/Ubuntu/\)](http://www.tothenew.com/blog/tag/ubuntu/)

FOUND THIS USEFUL? SHARE IT

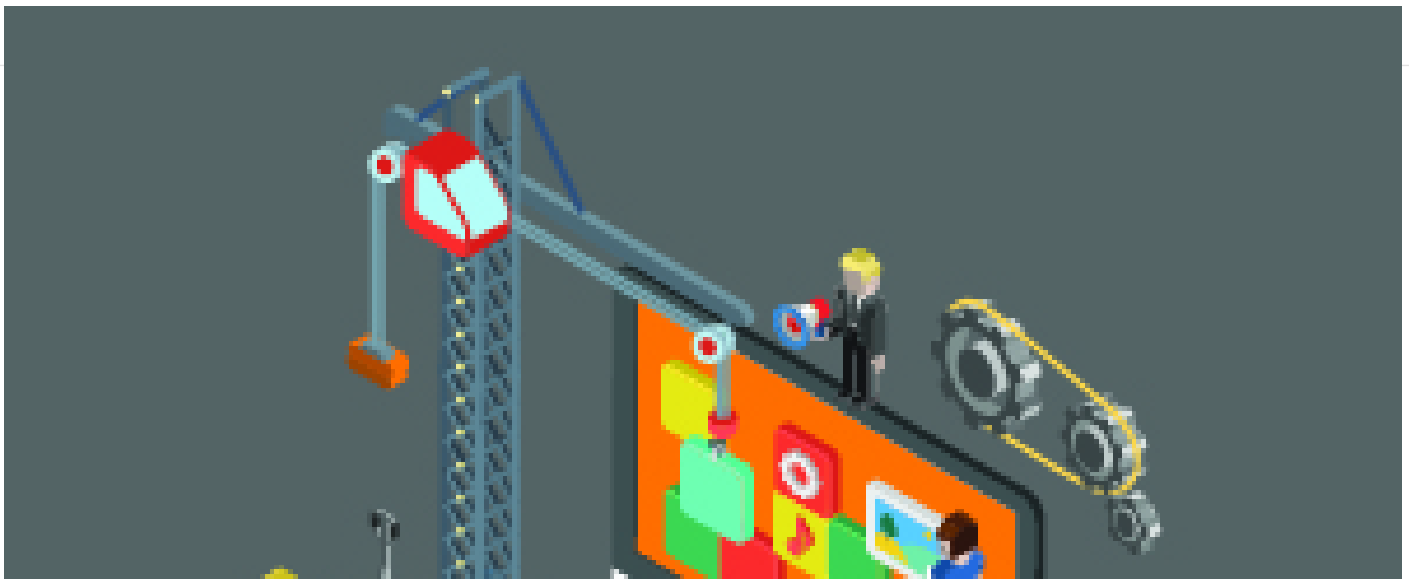
Email

Twitter

Facebook

LinkedIn

Google+





Whitepaper DevOps Practices and Principles To Improve IT Efficiency

Download Whitepaper (<http://insights.tothenew.com/devops-practices-principles-for-it-efficiency>)

LEAVE A COMMENT -

Name *

Email *

Comment

Submit



by

Ranvijay Jamwal (<http://www.tothenew.com/blog/author/ranvijayjintelligrape-com/>)


Ranvijay is a lead DevOps Engineer, accredited technical certified professional who has excellent ability to develop & implement technical solutions for any size of business and believes in learning each day. He is a charismatic and cheerful person who loves Linux shell scripting. Ranvijay believes that cloud and container technologies will bring about a revolution. He is also a Microsoft Certified Technology Associate. Besides he is a hardcore cricket fan, who has played state level matches and also loves singing and writing.

YOU MAY ALSO LIKE

Set-up SSL Communication between two Linux servers Using... (<http://www.tothenew.com/blog/set-up-ssl-communication-between-two-server-using-keytool-command/>)

Cgroups and Namespaces On Ubuntu (<http://www.tothenew.com/blog/cgroups-and-namespaces-on-ubuntu/>)

Install ngx_pagespeed module with nginx on ubuntu 14.04 (http://www.tothenew.com/blog/install-ngx_pagespeed-module-with-nginx-on-ubuntu-14-04/)



FOLLOW US ON

(https://www.facebook.com/tothenew) (https://www.instagram.com/tothenew) (https://twitter.com/tothenew) (https://www.youtube.com/channel/UCtTnNEW)



Subscribe to our Blog

Get latest articles straight to your inbox

Subscribe Now

- Who We Are +
- What We Do +
- Knowledge +
- Contact Us +
- Connect With Us