Configuration

Basic usage

Manager

Audit generates numerous events and it is hard to distinguish if those events correspond to a *write access*, *read access*, *execute access*, *attribute change*, or *system call rule*, using Wazuh decoders and rules. This is why we use the *key* argument in audit rules to facilitate the processing of events by Wazuh. As previously explained, each audit rule has the option to add a descriptive *key* value to identify what rule generated a particular audit log entry. We will use a CDB list to determine the types of audit rule that has fire. This list will have the following syntax:

```
key_name:value
```

where:

- **Key_name** is the string you used in the argument *-k* of a *file system rule* or a *call system rule*.
- **Value** is one of the following values:

  write: File system rules with -p **w**.

  read: File system rules with -p **r**.

  execute: File system rules with -p **x**.

  attribute: File system rules with -p **a**.

  command: System call rules.

By default, OSSEC includes a CDB list with the following keys:

```
$ cat /var/ossec/etc/lists/audit-keys

audit-wazuh-w:write
audit-wazuh-r:read
audit-wazuh-a:attribute
audit-wazuh-x:execute
audit-wazuh-c:command
```

You can add your own key with its value to the list like this:

```
echo "my_key_write_type:write" >> /var/ossec/etc/lists/audit-keys
```

Each time you modify a CDB list, you must compile it:

```
/var/ossec/bin/ossec-makelists
```

Agent

Installing Audit

In order to use the Audit system, you must have the audit package installed on your system. If you do not have this package installed, execute the following command as the root user to install it.

Red Hat, CentOS and Fedora:

```
$ yum install audit
```

Debian and Ubuntu based Linux distributions:

```
$ apt-get install auditd
```

Editing ossec.conf

Wazuh must be aware of the events detected by Audit. So, it is needs to be configured to read the audit log file:

```
<localfile>
  <log_format>audit</log_format>
  <location>/var/log/audit/audit.log</location>
</localfile>
```

Restarting OSSEC

Finally, we must restart Wazuh agent in order to apply the changes:

```
$ /var/ossec/bin/ossec-control restart
```

Now everything is ready to process audit events. You only need to create the proper audit rules (via *auditctl* or */etc/audit/audit.rules*). In the next section we will describe some good use cases.

Monitoring accesses to a directory

In this example, we are going to monitor every kind of access under the */home* directory:

```
auditctl -w /home -p w -k audit-wazuh-w
auditctl -w /home -p a -k audit-wazuh-a
auditctl -w /home -p r -k audit-wazuh-r
auditctl -w /home -p x -k audit-wazuh-x
```

Now we start getting alerts on account of the new audit rules:

```
** Alert 1487891035.24299: - audit,audit_configuration,
2017 Feb 23 15:03:55 localhost->/var/log/audit/audit.log
Rule: 80705 (level 3) -> 'Auditd: Configuration changed'
type=CONFIG_CHANGE msg=audit(1487891033.538:2936): auid=1000 ses=346
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op="add_rule" key="audit-wazuh-w" list=4 res=1
audit.type: CONFIG_CHANGE
audit.id: 2936
audit.key: audit
audit.list: 4
audit.res: 1

** Alert 1487891043.24730: - audit,audit_configuration,
2017 Feb 23 15:04:03 localhost->/var/log/audit/audit.log
Rule: 80705 (level 3) -> 'Auditd: Configuration changed'
type=CONFIG_CHANGE msg=audit(1487891041.427:2937): auid=1000 ses=346
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op="add_rule" key="audit-wazuh-a" list=4 res=1
audit.type: CONFIG_CHANGE
audit.id: 2937
audit.key: audit
audit.list: 4
audit.res: 1
```

```
** Alert 1487891047.25161: - audit,audit_configuration,
2017 Feb 23 15:04:07 localhost->/var/log/audit/audit.log
Rule: 80705 (level 3) -> 'Auditd: Configuration changed'
type=CONFIG_CHANGE msg=audit(1487891045.481:2938): auid=1000 ses=346
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op="add_rule" key="audit-wazuh-r" list=4 res=1
audit.type: CONFIG_CHANGE
audit.id: 2938
audit.key: audit
audit.list: 4
audit.res: 1

** Alert 1487891049.25592: - audit,audit_configuration,
2017 Feb 23 15:04:09 localhost->/var/log/audit/audit.log
Rule: 80705 (level 3) -> 'Auditd: Configuration changed'
type=CONFIG_CHANGE msg=audit(1487891049.144:2939): auid=1000 ses=346
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op="add_rule" key="audit-wazuh-x" list=4 res=1
audit.type: CONFIG_CHANGE
audit.id: 2939
audit.key: audit
audit.list: 4
audit.res: 1
```

Note

While it would be possible to define the previous rules as one single rule that specifies *-p warx*, we intentionally separate them out so each rule has its own unique **key** value that is important for analysis.

Let's see what happens when we execute the following commands:

New File

Command:

```
$ touch /home/malware.py
```

Alert:

```
** Alert 1487891161.28457: - audit,audit_watch_write,audit_watch_create,
2017 Feb 23 15:06:01 localhost->/var/log/audit/audit.log
Rule: 80790 (level 3) -> 'Audit: Created: /home/malware.py'
type=SYSCALL msg=audit(1487891161.190:2942): arch=c000003e syscall=2 success=yes exit=3 a0=7ffce677b7b7
a1=941 a2=1b6 a3=7ffce6779690 items=2 ppid=60621 pid=60761 auid=1000 uid=0 gid=0 euid=0 suid=0
fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=346 comm="touch" exe="/usr/bin/touch"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="audit-wazuh-w" type=CWD
msg=audit(1487891161.190:2942):  cwd="/" type=PATH msg=audit(1487891161.190:2942): item=0
name="/home/" inode=16777403 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00
obj=system_u:object_r:home_root_t:s0 objtype=PARENT type=PATH msg=audit(1487891161.190:2942):item=1
name="/home/malware.py" inode=18369115 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00
obj=unconfined_u:object_r:home_root_t:s0 objtype=CREATE
audit.type: SYSCALL
audit.id: 2942
audit.syscall: 2
audit.success: yes
audit.exit: 3
audit.ppid: 60621
audit.pid: 60761
audit.auid: 1000
audit.uid: 0
audit.gid: 0
audit.euid: 0
audit.suid: 0
audit.fsuid: 0
audit.egid: 0
audit.sgid: 0
audit.fsgid: 0
audit.tty: pts0
audit.session: 346
audit.command: touch
audit.exe: /usr/bin/touch
audit.key: audit-wazuh-w
audit.cwd: /
audit.directory.name: /home/
audit.directory.inode: 16777403
audit.directory.mode: 040755
audit.file.name: /home/malware.py
audit.file.inode: 18369115
audit.file.mode: 0100644
```

Write Access

Command:

```
$ nano /home/malware.py
```

Alert:

```
** Alert 1487891353.48010: - audit,audit_watch_write,
2017 Feb 23 15:09:13 localhost->/var/log/audit/audit.log
Rule: 80781 (level 3) -> 'Audit: Watch - Write access: /home/malware.py'
type=SYSCALL msg=audit(1487891353.291:2956): arch=c000003e syscall=2 success=yes exit=3 a0=9e2e80
a1=441 a2=1b6 a3=63 items=2 ppid=60621 pid=60819 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
sgid=0 fsgid=0 tty=pts0 ses=346 comm="nano" exe="/usr/bin/nano"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="audit-wazuh-w"
type=CWD msg=audit(1487891353.291:2956):  cwd="/" type=PATH msg=audit(1487891353.291:2956): item=0
name="/home/" inode=16777403 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00
obj=system_u:object_r:home_root_t:s0 objtype=PARENT type=PATH msg=audit(1487891353.291:2956): item=1
name="/home/malware.py" inode=18369115 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00
obj=unconfined_u:object_r:home_root_t:s0 objtype=NORMAL
audit.type: SYSCALL
audit.id: 2956
audit.syscall: 2
audit.success: yes
audit.exit: 3
audit.ppid: 60621
audit.pid: 60819
audit.auid: 1000
audit.uid: 0
audit.gid: 0
audit.euid: 0
audit.suid: 0
audit.fsuid: 0
audit.egid: 0
audit.sgid: 0
audit.fsgid: 0
audit.tty: pts0
audit.session: 346
audit.command: nano
audit.exe: /usr/bin/nano
audit.key: audit-wazuh-w
audit.cwd: /
audit.directory.name: /home/
audit.directory.inode: 16777403
audit.directory.mode: 040755
audit.file.name: /home/malware.py
audit.file.inode: 18369115
audit.file.mode: 0100644
```

Change Permissions

Command:

```
$ chmod u+x /home/malware.py
```

Alert:

```
** Alert 1487891409.49498: - audit,audit_watch_attribute,
2017 Feb 23 15:10:09 localhost->/var/log/audit/audit.log
Rule: 80787 (level 3) -> 'Audit: Watch - Change attribute: /home/malware.py'
type=SYSCALL msg=audit(1487891408.563:2957): arch=c000003e syscall=268 success=yes exit=0
a0=ffffffffffffff9c
a1=22f50f0 a2=1e4 a3=7fffe879a7d0 items=1 ppid=60621 pid=60820 auid=1000 uid=0 gid=0 euid=0
suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=346 comm="chmod" exe="/usr/bin/chmod"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="audit-wazuh-a" type=CWD
msg=audit(1487891408.563:2957):  cwd="/" type=PATH msg=audit(1487891408.563:2957): item=0
name="/home/malware.py" inode=18369115 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00
obj=unconfined_u:object_r:home_root_t:s0 objtype=NORMAL
audit.type: SYSCALL
audit.id: 2957
audit.syscall: 268
audit.success: yes
audit.exit: 0
audit.ppid: 60621
audit.pid: 60820
audit.auid: 1000
audit.uid: 0
audit.gid: 0
audit.euid: 0
audit.suid: 0
audit.fsuid: 0
audit.egid: 0
audit.sgid: 0
audit.fsgid: 0
audit.tty: pts0
audit.session: 346
audit.command: chmod
audit.exe: /usr/bin/chmod
audit.key: audit-wazuh-a
audit.cwd: /
audit.file.name: /home/malware.py
audit.file.inode: 18369115
audit.file.mode: 0100644
```

Read access

Command:

```
$ /home/malware.py
```

Alert:

```
** Alert 1487891459.53222: - audit,audit_watch_read,
2017 Feb 23 15:10:59 localhost->/var/log/audit/audit.log
Rule: 80784 (level 3) -> 'Audit: Watch - Read access: /home/malware.py'
type=SYSCALL msg=audit(1487891458.283:2960): arch=c000003e syscall=2 success=yes exit=3 a0=14d1e20
a1=0 a2=ffffffffffffff80 a3=7ffdd01083d0 items=1 ppid=60621 pid=60821 auid=1000 uid=0 gid=0 euid=0
suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=346 comm="bash" exe="/usr/bin/bash"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="audit-wazuh-r" type=CWD
msg=audit(1487891458.283:2960):  cwd="/" type=PATH msg=audit(1487891458.283:2960): item=0
name="/home/malware.py" inode=18369115 dev=fd:00 mode=0100744 ouid=0 ogid=0 rdev=00:00
obj=unconfined_u:object_r:home_root_t:s0 objtype=NORMAL
audit.type: SYSCALL
audit.id: 2960
audit.syscall: 2
audit.success: yes
audit.exit: 3
audit.ppid: 60621
audit.pid: 60821
audit.auid: 1000
audit.uid: 0
audit.gid: 0
audit.euid: 0
audit.suid: 0
audit.fsuid: 0
audit.egid: 0
audit.sgid: 0
audit.fsgid: 0
audit.tty: pts0
audit.session: 346
audit.command: bash
audit.exe: /usr/bin/bash
audit.key: audit-wazuh-r
audit.cwd: /
audit.file.name: /home/malware.py
audit.file.inode: 18369115
audit.file.mode: 0100744
```

Delete file

Command:

```
$ rm /home/malware.py
```

Alert:

```
** Alert 1487891497.54463: - audit,audit_watch_write,audit_watch_delete,
2017 Feb 23 15:11:37 localhost->/var/log/audit/audit.log
Rule: 80791 (level 3) -> 'Audit: Deleted: /home/malware.py'
type=SYSCALL msg=audit(1487891496.026:2961): arch=c000003e syscall=263 success=yes exit=0
a0=ffffffffffffff9c a1=13b00c0 a2=0 a3=7ffe1b582dc0 items=2 ppid=60621 pid=60824 auid=1000
uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=346 comm="rm" exe="/usr/bin/rm"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="audit-wazuh-w"
type=CWD msg=audit(1487891496.026:2961):  cwd="/" type=PATH msg=audit(1487891496.026:2961): item=0
name="/home/" inode=16777403 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00
obj=system_u:object_r:home_root_t:s0 objtype=PARENT type=PATH msg=audit(1487891496.026:2961): item=1
name="/home/malware.py" inode=18369115 dev=fd:00 mode=0100744 ouid=0 ogid=0 rdev=00:00
obj=unconfined_u:object_r:home_root_t:s0 objtype=DELETE
audit.type: SYSCALL
audit.id: 2961
audit.syscall: 263
audit.success: yes
audit.exit: 0
audit.ppid: 60621
audit.pid: 60824
audit.auid: 1000
audit.uid: 0
audit.gid: 0
audit.euid: 0
audit.suid: 0
audit.fsuid: 0
audit.egid: 0
audit.sgid: 0
audit.fsgid: 0
audit.tty: pts0
audit.session: 346
audit.command: rm
audit.exe: /usr/bin/rm
audit.key: audit-wazuh-w
audit.cwd: /
audit.directory.name: /home/
audit.directory.inode: 16777403
audit.directory.mode: 040755
audit.file.name: /home/malware.py
audit.file.inode: 18369115
audit.file.mode: 0100744
```

Monitoring user actions

Here we choose to audit all commands run by a user who has admin privileges. The audit configuration for this is quite simple:

```
$ auditctl -a exit,always -F euid=0 -F arch=b64 -S execve -k audit-wazuh-c
$ auditctl -a exit,always -F euid=0 -F arch=b32 -S execve -k audit-wazuh-c
```

If the root user executes nano, the alert will look like this:

```
** Alert 1487892032.56406: - audit,audit_command,
2017 Feb 23 15:20:32 localhost->/var/log/audit/audit.log
Rule: 80792 (level 3) -> 'Audit: Command: /usr/bin/nano'
type=SYSCALL msg=audit(1487892031.893:2963): arch=c000003e syscall=59 success=yes exit=0 a0=14e4990
a1=14e4a30 a2=14d4ef0 a3=7ffdd01083d0 items=2 ppid=60621 pid=60840 auid=1000 uid=0 gid=0 euid=0
suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=346 comm="nano" exe="/usr/bin/nano"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="audit-wazuh-c" type=EXECVE
msg=audit(1487892031.893:2963): argc=1 a0="nano" type=CWD msg=audit(1487892031.893:2963):
cwd="/" type=PATH msg=audit(1487892031.893:2963): item=0 name="/bin/nano" inode=18372489 dev=fd:00
mode=0100755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:bin_t:s0 objtype=NORMAL type=PATH
msg=audit(1487892031.893:2963): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=33595530 dev=fd:00
mode=0100755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:ld_so_t:s0 objtype=NORMAL
audit.type: SYSCALL
audit.id: 2963
audit.syscall: 59
audit.success: yes
audit.exit: 0
audit.ppid: 60621
audit.pid: 60840
audit.auid: 1000
audit.uid: 0
audit.gid: 0
audit.euid: 0
audit.suid: 0
audit.fsuid: 0
audit.egid: 0
audit.sgid: 0
audit.fsgid: 0
audit.tty: pts0
audit.session: 346
audit.command: nano
audit.exe: /usr/bin/nano
audit.key: audit-wazuh-c
audit.cwd: /
audit.file.name: /bin/nano
audit.file.inode: 18372489
audit.file.mode: 0100755
```

Privilege escalation

By default, Wazuh is able to detect privilege escalation by analyzing the corresponding log in */var/log/auth.log*. The below example shows the homer user executing a root action:

```
$ homer@springfield:/$ sudo ls /var/ossec/etc
```

Wazuh detects the action, extracting the *srcuser*, *dstuser* and *command* among other fields:

```
** Alert 1487892460.79075: - syslog,sudo,pci_dss_10.2.5,pci_dss_10.2.2,
2017 Feb 23 15:27:40 localhost->/var/log/secure
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed'
User: root
Feb 23 15:27:40 localhost sudo:    rromero : TTY=pts/0 ; PWD=/home/rromero ; USER=root ; COMMAND=/bin/ls
/var/ossec/etc
tty: pts/0
pwd: /home/rromero
command: /bin/ls
```

However, you may find this level of detail inadequate, in which case you can use Audit.

If you have created a rule to monitor root actions, like in the previous use case, every action with *sudo* will be logged, but the **auid** field will inconveniently be 0 (root user) instead of that of the actual user who initiated the escalated action. You generally want to know who originally initiated a command, regardless of if it was escalated or not.

In order to keep the track of the user after sudo, it is necessary to configure *PAM*.

> **⚠ Warning**
>
> Be very careful with PAM configuration, as a bad configuration could make your system inaccessible.

Add the following line to every PAM service that needs it:

```
session required        pam_loginuid.so
```

A common configuration should include: *login*, *common-session*, *cron* and *sshd*:

```
$ grep -R "pam_loginuid.so" /etc/pam.d/

/etc/pam.d/login:session    required     pam_loginuid.so
/etc/pam.d/common-session:session required        pam_loginuid.so
/etc/pam.d/cron:session    required     pam_loginuid.so
/etc/pam.d/sshd:session    required     pam_loginuid.so
```

After configuring PAM, if we execute the previous command with the user *homer* we will see that the field *auid* is 1004, the id of the user homer.

```
$ homer@springfield:/$ sudo ls /var/ossec/etc
```

```
** Alert 1487892803.121460: - audit,audit_command,
2017 Feb 23 15:33:23 localhost->/var/log/audit/audit.log
Rule: 80792 (level 3) -> 'Audit: Command: /usr/bin/ls'
type=SYSCALL msg=audit(1487892802.652:3054): arch=c000003e syscall=59 success=yes exit=0 a0=7f711f7d4ef8
a1=7f711f7d6358 a2=7f711f7df2e0 a3=7 items=2 ppid=60910 pid=60911 auid=1000 uid=0 gid=0 euid=0 suid=0
fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=346 comm="ls" exe="/usr/bin/ls"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="audit-wazuh-c" type=EXECVE
msg=audit(1487892802.652:3054): argc=2 a0="ls" a1="/var/ossec/etc" type=CWD msg=audit(1487892802.652:3054):
cwd="/home/rromero" type=PATH msg=audit(1487892802.652:3054): item=0 name="/bin/ls" inode=16912203 dev=fd:00
mode=0100755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:bin_t:s0 objtype=NORMAL type=PATH
msg=audit(1487892802.652:3054): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=33595530 dev=fd:00
mode=0100755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:ld_so_t:s0 objtype=NORMAL
audit.type: SYSCALL
audit.id: 3054
audit.syscall: 59
audit.success: yes
audit.exit: 0
audit.ppid: 60910
audit.pid: 60911
audit.auid: 1000
audit.uid: 0
audit.gid: 0
audit.euid: 0
audit.suid: 0
audit.fsuid: 0
audit.egid: 0
audit.sgid: 0
audit.fsgid: 0
audit.tty: pts0
audit.session: 346
audit.command: ls
audit.exe: /usr/bin/ls
audit.key: audit-wazuh-c
audit.cwd: /home/rromero
audit.file.name: /bin/ls
audit.file.inode: 16912203
audit.file.mode: 0100755
```