



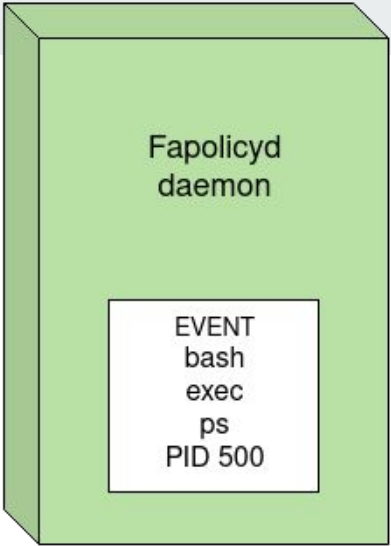
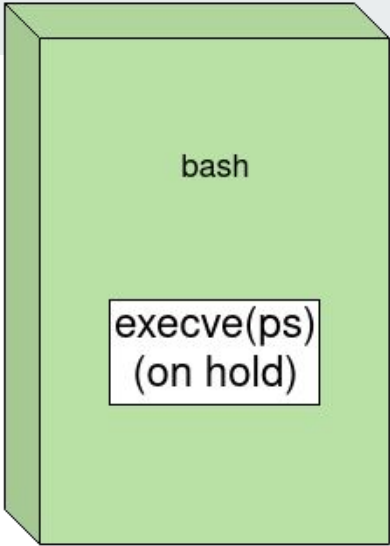
# Fapolicyd Framework

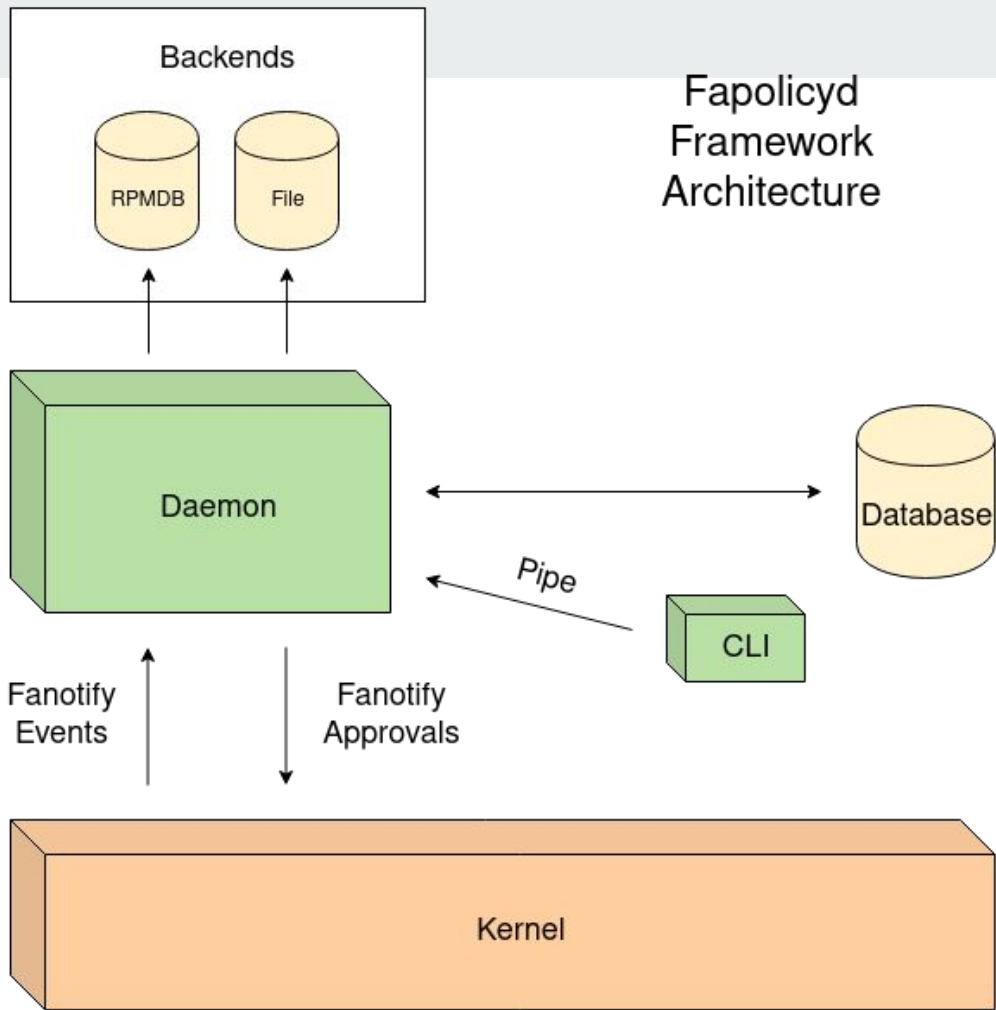
- Lightweight solution
- RPM/DNF integration
- Audit support
- Relies on fanotify API



# Fanotify API

- Kernel API
- Similar to inotify
- Receiving events from open/exec system calls
- Blockable on system call side, waiting for response







# Fapolicyd Configuration

- `/etc/fapolicyd/`
  - `fapolicyd.rules`
  - `fapolicyd.conf`
  - `fapolicyd.trust`



# Fapolicyd Trust Philosophy

- Optional backends
- By default (RHEL/Fedora) everything loaded from
  - rpmdb
  - fapolicyd.trust
- is trusted
- The default set of rules ensures that trusted application is allowed to run



# Rule language

- Subject/Object notation



# Simple format

DECISION PERM SUBJECT : OBJECT





# Decision

- allow
- allow\_audit
- deny
- deny\_audit



# Permission

- open
- execute
- any



# Simple format

DECISION PERM SUBJECT : OBJECT



# Install Fapolicyd Framework

```
[root@Axis ~] dnf install fapolicyd
```



# Enable Apps In Home Directory

Problem:

- Regular user would like to run his software in ~/bin
  - Enable binary
  - Enable python script



# Enable Specific Binary

- ~/bin/my-bin

```
~/bin >> ls  
my-bin my-app.py
```

```
~/bin >> ./my-bin  
my-bin my-app.py
```



# Running Daemon In Debug Mode

```
[root@Axis ~]# fapolicyd --debug 2>&1 | tee out
Loaded 24 rules
Changed to uid 980
Initializing the database
Loading rpmdb backend
Loading file backend
Checking database
...
Starting to listen for events
...
```



# Enable Specific Binary

- ~/bin/my-bin

```
~/bin >> ls  
my-bin my-app.py
```

```
~/bin >> ./my-bin  
Zsh: operation not permitted:  
./my-bin
```





# Output Investigation

```
[root@Axis ~]# less out
```

```
Loaded 24 rules  
Changed to uid 980  
Initializing the database  
Loading rpmdb backend  
Loading file backend  
Checking database  
...  
Starting to listen for events  
/my-bin
```



# Output Investigation

```
rule:9 dec=deny audit perm=execute auid=1000 pid=600 exe=/usr/bin/zsh  
: file=/home/rsroka/bin/my-bin ftype=application/x-executable
```



# Output Investigation

```
rule:9 dec=deny audit perm=execute auid=1000 pid=600 exe=/usr/bin/zsh  
: file=/home/rsroka/bin/my-bin ftype=application/x-executable
```

Rule:

```
allow perm=execute exe=/usr/bin/zsh trust=1  
: file=/home/rsroka/bin/my-bin ftype=application/x-executable trust=0
```



# Enable Specific Binary

- ~/bin/my-bin

```
~/bin >> ls  
my-bin my-app.py
```

```
~/bin >> ./my-bin  
my-bin my-app.py
```



# Enable Python Script

- ~/bin/my-app.py

```
~/bin >> ls  
my-bin my-app.py
```

```
~/bin >> ./my-app.py  
Hello World from Python Script
```



# Running Daemon In Debug Mode

```
[root@Axis ~]# fapolicyd --debug 2>&1 | tee out
Loaded 24 rules
Changed to uid 980
Initializing the database
Loading rpmdb backend
Loading file backend
Checking database
...
Starting to listen for events
...
```



# Enable Python Script

- ~/bin/my-app.py

```
~/bin >> ls  
my-bin my-app.py
```

```
~/bin >> ./my-app.py  
zsh: operation not permitted:  
my-app.py
```



# Output Investigation

```
[root@Axis ~]# less out
```

```
Loaded 24 rules  
Changed to uid 980  
Initializing the database  
Loading rpmdb backend  
Loading file backend  
Checking database  
...  
Starting to listen for events  
/my-app
```





# Output Investigation

```
rule:9 dec=deny audit perm=execute auid=1000 pid=600 exe=/usr/bin/zsh  
: file=/home/rsroka/bin/my-app.py ftype=text/x-python
```



# Output Investigation

```
rule:9 dec=deny audit perm=execute auid=1000 pid=600 exe=/usr/bin/zsh  
: file=/home/rsroka/bin/my-app.py ftype=text/x-python
```

Rule:

```
allow perm=execute exe=/usr/bin/zsh trust=1  
: file=/home/rsroka/bin/my-app.py ftype=text/x-python trust=0
```




# Enable Python Script

- ~/bin/my-app.py

```
~/bin >> ls  
my-bin my-app.py
```


```
~/bin >> ./my-app.py  
zsh: operation not permitted:  
my-app.py
```

Wait...What?



## Output Investigation - The Second Round

```
rule:2 dec=allowed perm=execute auid=1000 pid=600 exe=/usr/bin/zsh :  
file=/home/rsroka/bin/my-app.py ftype=text/x-python  
  
rule:18 dec=deny audit perm=open auid=1000 pid=600 exe=/usr/bin/zsh :  
file=/home/rsroka/bin/my-app.py ftype=text/x-python
```



## Output Investigation - The Second Round

```
rule:2 dec=allowed perm=execute auid=1000 pid=600 exe=/usr/bin/zsh :  
file=/home/rsroka/bin/my-app.py ftype=text/x-python  
  
rule:18 dec=deny audit perm=open auid=1000 pid=600 exe=/usr/bin/zsh :  
file=/home/rsroka/bin/my-app.py ftype=text/x-python
```

Rule:

```
allow perm=any exe=/usr/bin/zsh trust=1  
: file=/home/rsroka/bin/my-app.py ftype=text/x-python trust=0
```




# Enable Python Script

- ~/bin/my-app.py

```
~/bin >> ls  
my-bin my-app.py
```

```
~/bin >> ./my-app.py  
Hello World from Python Script
```

```
~/bin >> python3 my-app.py  
Hello World from Python Script
```



```
rule:2 dec=allowed perm=execute exe=/usr/bin/zsh :  
file=/home/rsroka/bin/my-app.py ftype=text/x-python  
  
rule:2 dec=allowed perm=execute exe=/usr/bin/python3.7 :  
file=/home/rsroka/bin/my-app.py ftype=text/x-python
```

### Rule:

```
allow perm=any all trust=1  
: file=/home/rsroka/bin/my-app.py ftype=text/x-python trust=0
```



# Enable Directory

```
allow perm=any all trust=1 : dir=/home/rsroka/bin/ trust=0
```





# Mark Files As Trusted

- Add files to fapolicyd.trust

```
# FULL PATH SIZE SHA256  
/home/rsroka/bin/my-bin 15523 61a9960bf7d255a85811f4afcac51062e...  
/home/rsroka/bin/my-app.py 153 e49f0c887cf5fd41d4d49808fc8042fc...
```



# Enable Fapolicyd Framework

```
[root@Axis ~] systemctl enable --now fapolicyd
```



# Thank You!

- [rsroka@redhat.com](mailto:rsroka@redhat.com)
- <https://github.com/radosroka>
- <https://twitter.com/RadovanSroka>
- <https://github.com/linux-application-whitelisting/fapolicyd>