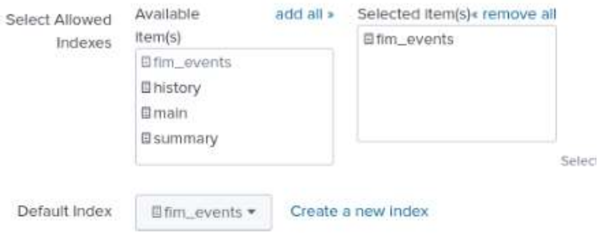
Installing FileIntegrityMonitoring

Sunday, February 04, 2024 7:25 PM

Print documentation.achiefs.com/docs/installation-guide.html

Splunk Integration

- Splunk home page > Settings > Data – Indexes
- New index
- Index Name: fim_events > Save
- Settings > Data – Data Inputs
- Add new http event collector
- Name: FIMCollector
- Input Settings should look like this



Select Allowed Indexes

Available item(s) — add all »
- fim_events
- history
- main
- summary

Selected item(s) « remove all
- fim_events

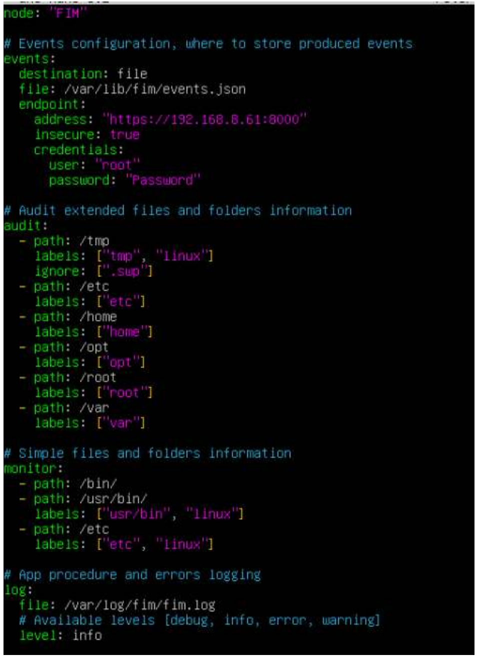
Selec

Default Index: fim_events ▾ — Create a new index

- Review > Submit > Copy token value

Debian

- wget https://github.com/Achiefs/fim/releases/download/v0.4.10/fim_0.4.10-1_amd64.deb
- sudo dpkg -i fim*.deb
- sudo systemctl start fim
- sudo systemctl status fim
- sudo nano /etc/fim/config.yml



```
node: "FIM"

# Events configuration, where to store produced events
events:
  destination: file
  file: /var/lib/fim/events.json
  endpoint:
    address: "https://192.168.8.61:8000"
    insecure: true
    credentials:
      user: "root"
      password: "Password"

# Audit extended files and folders information
audit:
  - path: /tmp
    labels: ["tmp", "linux"]
    ignore: [".swp"]
  - path: /etc
    labels: ["etc"]
  - path: /home
    labels: ["home"]
  - path: /opt
    labels: ["opt"]
  - path: /root
    labels: ["root"]
  - path: /var
    labels: ["var"]

# Simple files and folders information
monitor:
  - path: /bin/
  - path: /usr/bin/
    labels: ["usr/bin", "linux"]
  - path: /etc
    labels: ["etc", "linux"]

# App procedure and errors logging
log:
  file: /var/log/fim/fim.log
  # Available levels [debug, info, error, warning]
  level: info
```

- Any red in the config is bad, green is good
- The credentials are for splunk

Print