

Monitoring system calls

The [Linux Audit system](#) provides a way to track security-relevant information on your machine. Based on preconfigured rules, Audit proves detailed real-time logging about the events that are happening on your system. This information is crucial for mission-critical environments to determine the violator of the security policy and the actions they performed.

Contents

- [How it works](#)
 - [Control rules](#)
 - [File System Rules](#)
 - [System Call Rules](#)
- [Configuration](#)
 - [Basic usage](#)
 - [Monitoring accesses to a directory](#)
 - [Monitoring user actions](#)
 - [Privilege escalation](#)

