Chemnitzer Linux-Tage 2022

Kurz-Paper zum Vortrag „`setenforce 1`“

Florian Winkler

Standardvortrag (ca. 45 Minuten & 10 Minuten Diskussion)

Abstract

SELinux, ursprünglich ein Forschungsprojekt der NSA, ist eine Architektur zur Umsetzung von Mandatory Access Control zur Erweiterung des bestehenden Sicherheitssystems in Linux. Im Jahr 2000 als Open Source veröffentlicht und seit Version 2.6 fester Bestandteil des Kernels wird SELinux vor allem von Red Hat eingesetzt und weiterentwickelt. Dabei bietet SELinux feingranulare Regeln zur Zugriffssteuerung. Damit einhergehend ist aber auch eine große Komplexität, die sehr häufig zur Abschaltung von SELinux führt. Dort setzt dieser Vortrag an und zeigt die wichtigsten Begriffe, Tools und Möglichkeiten zum Debugging von SELinux. Mit Hilfe von praxisnahen Beispielen werden die Grundlagen der Konfiguration demonstriert, um effektiv mit SELinux im „enforcing"-Modus zu arbeiten.

Zielgruppe

Sicherheitsbewusste Linux-Anwendende und -Administrierende

Benötigte Vorkenntnisse

Linux-Grundlagen, insbesondere zur Arbeit in der Shell, der Benutzer- und Rechteverwaltung

Zusatzinformationen zum Vortrag

Nach einem kurzen Einblick in die Historie von SELinux und der Klärung, wozu SELinux eingesetzt werden kann, wird die Architektur näher beleuchtet. Es folgt die Vorstellung der wichtigsten Fachbegriffe sowie der wichtigsten Tools rund um SELinux. Abgerundet wird das ganze durch praxisnahe Beispiele, um den Zuhörenden die Konfiguration und den Einsatz von SELinux näher zu bringen. Dabei werden alltägliche Administrationsaufgaben dargestellt und so Berührungsängste mit der komplexen Materie abgebaut und Grundlagen geschaffen, um das Gelernte zügig selbständig umsetzen zu können.

Vorgestellte Begriffe und Werkzeuge (unvollständig)

Mandatory/Discretionary Access Control, SELinux, `sestatus`, `seinfo`, Targeted Policy, AVC, `auditd`, `getenforce`, `setenforce`, Domain, Context, `getsebool`, `setsebool`, `fixfiles`, `restorecon`, `chcon`, `semanage`, `audit2allow`, `/etc/selinux/`, `/var/log/audit.log`

Weiterführende Links

- `https://www.redhat.com/en/topics/linux/what-is-selinux`
- `https://selinuxproject.org/page/Main_Page`
- `https://wiki.centos.org/HowTos/SELinux`
- `https://codingbee.net/rhcsa/rhcsa-selinux-overview`