

disable auditing of TTY input for specified users. When the audited user logs in, pam_tty_audit records the exact keystrokes the user makes into the /var/log/audit/audit.log file. The module works with the audited daemon, so make sure it is enabled before configuring pam_tty_audit. See Section 7.4, "Starting the audit Service" for more information.

When you want to specify user names for TTY auditing, modify the /etc/pam.d/system-auth and /etc/pam.d/password-auth files using the disable and enable options in the following format:

session required pam_tty_audit.so disable=username,username2 enable=username

You can specify one or more user names separated by commas in the options. Any disable or enable option overrides the previous opposite option which matches the same user name. When TTY auditing is enabled, it is inherited by all processes started by that user. In particular, daemons restarted by a user will still have TTY auditing enabled, and will audit TTY input even by other users,

unless auditing for these users is explicitly disabled. Therefore, it is recommended to use disable=* as the first option for most daemons using PAM.

Important



Use By default, <code>pam_tty_audit</code> does **NOT** log keystrokes when the TTY is in password entry mode. Logging can be reenabled by adding the log passwd option along with the other options in the following way:

session required pam_tty_audit.so disable=username,username2 enable=username log passwd

When you enable the module, the input is logged in the /var/log/audit/audit.log file, written by the audita daemon. Note that the input is not logged immediately, because TTY auditing first stores the keystrokes in a buffer and writes the record periodically, or once the audited user logs out. The audit.log file contains all keystrokes entered by the specified user, including backspaces, delete and return keys, the control key and others. Although the contents of audit.log are human-readable it might be easier to use the aureport utility, which provides a TTY report in a format which is easy to read. You can use the following command as root:

```
~]# aureport --tty
```

The following is an example of how to configure pam_tty_audit to track the actions of the root user across all terminals and then review the input.

Example 7.8. Configuring pam_tty_audit to log root actions

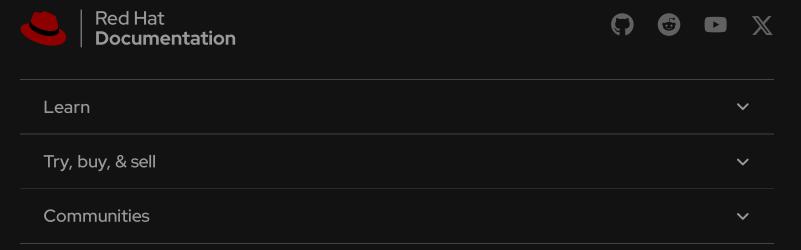
Enter the following line in the session section of the /etc/pam.d/system-auth and /etc/pam.d/password-auth files:

7.9. Configuring PAM for Auditing | Red Hat Product Documentation - 31/10/2024 14:43

https://docs.redhat.com/en/documentation/red hat enterprise linux/6/html/security guide/sec-configuring pam for auditing

For more information, see the pam_tty_audit(8) manual page.

Previous Next



About Red Hat Documentation

We help Red Hat users innovate and achieve their goals with our products and services with content they can trust.

7.9. Configuring PAM for Auditing | Red Hat Product Documentation - 31/10/2024 14:43

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/6/html/security_guide/sec-configuring_pam_for_auditing

Making open source more inclusive

Red Hat is committed to replacing problematic language in our code, documentation, and web properties For more details, see the <u>Red Hat Blog</u>.

About Red Hat

We deliver hardened solutions that make it easier for enterprises to work across platforms and environments, from the core datacenter to the network edge.



About Red Hat Jobs Even

Locations Contact Red Hat Red Hat Blog

Diversity, equity, and inclusion Cool Stuff Store Red Hat Summit

© 2024 Red Hat, Inc.

Privacy statement Terms of use All policies and guidelines

Digital accessibility Cookie preferences