LOGZILLA DOCUMENTATION

Linux PAM

Rules, dashboards, and triggers for Linux Pluggable Authentication Modules (PAM)

LogZilla App Store · Generated June 12, 2026 · logzilla.ai/docs/logzilla-appstore/linux—pam

Overview

Linux Pluggable Authentication Modules (PAM) is a suite of libraries that allows system administrators to configure authentication methods for users. PAM provides a flexible and centralized way to manage authentication across secured applications and services.

App Function

- Parse `pam_unix` authentication log messages
- Extract session events (opened/closed) and authentication failures
- Track users, remote hosts, and TTY devices
- Set `Vendor: Linux` and `Product: PAM` tags for filtering
- Categorize events with `Event Class: auth`
- Alert on authentication failures and root session access

Vendor Documentation

- Linux-PAM Website (http://www.linux-pam.org/)
- Linux PAM - ArchWiki (https://wiki.archlinux.org/title/PAM)
- Introduction to PAM (https://www.redhat.com/sysadmin/pluggable-authentication-modules-pam)

Device Configuration

PAM log messages are written to `/var/log/auth.log` (Debian/Ubuntu) or `/var/log/secure` (RHEL/CentOS). Configure syslog forwarding to send these logs to LogZilla:

Edit the syslog configuration (e.g., `/etc/rsyslog.d/logzilla.conf`)

Add a rule to forward auth logs:

```
auth,authpriv.*    @logzilla-server:514
```

Restart the syslog service:

```
sudo systemctl restart rsyslog
```

Verification

Trigger an authentication event (e.g., SSH login) and verify events appear in LogZilla with the message containing `pam_unix`.

Incoming Log Format

PAM log messages follow this format:

```
pam_unix(<process>:<context>): <message>
```

- **process** - Service name (sshd, sudo, login, systemd-user)
- **context** - PAM context (session, auth)
- **message** - Event description

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Linux	Vendor name
Product	PAM	Product name
Event Class	auth	Cross-vendor event classification
Event Type	login_failure	Specific event type (login_failure, session_start, session_end)
PAM Action	session opened	Authentication action or failure message
PAM User Tracking	vmuser	User being authenticated
User	vmuser	Username (same as PAM User Tracking)
Process	sshd	Process handling the session
Status	opened	Session status
PAM TTY	ssh	Terminal device (auth failures only)
PAM Remote Host	192.168.250.2	Remote host address (auth failures only)

Tag Name	Example	Description
PAM Remote User	admin	Remote username (auth failures only)
DstIP	10.0.0.1	Destination IP address (session logs)

Log Examples

Session Opened

```
pam_unix(sshd:session): session opened for user vmuser by (uid=0)
```

Session Closed

```
pam_unix(sudo:session): session closed for user root
```

Authentication Failure

```
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=192.168.250.2  user=vmuser
```

Triggers

Trigger	Description
PAM: Authentication Failure	Authentication failures - potential brute force
PAM: Root Session Opened	Root session opened - privilege escalation monitoring