LOGZILLA DOCUMENTATION

Linux

LogZilla App Store application: Linux

LogZilla App Store · Generated May 3, 2026 · logzilla.ai/docs/logzilla-appstore/linux

Overview

Linux is an open-source operating system kernel that forms the foundation of many server and desktop distributions. The Linux app handles core Linux system services including SSH authentication, privilege escalation (sudo/su/dzdo), scheduled tasks (cron), and service management (systemd).

App Function

- Parse sshd, sudo, su, dzdo (Centrify), cron, and systemd log messages
- Extract user, source IP, command, and service metadata
- Categorize events by Event Class (auth, system)
- Map security events to MITRE ATT&CK techniques
- Provide dashboards for authentication and system monitoring
- Alert on authentication failures and privilege escalation

Vendor Documentation

- OpenSSH sshd Manual (https://man.openbsd.org/sshd.8) - SSH daemon configuration
- OpenSSH Logging (https://man.openbsd.org/sshd_config#LogLevel) - SSH log levels
- sudo Manual (https://www.sudo.ws/docs/man/sudo.man/) - Privilege escalation
- Delinea dzdo (https://docs.delinea.com/) - Centrify/Delinea privilege escalation
- systemd Logging (https://systemd.io/) - Service and journal logging
- cron Manual (https://man7.org/linux/man-pages/man8/cron.8.html) - Scheduled tasks

Device Configuration

Configure Linux to forward syslog messages to LogZilla. Replace `LOGZILLA_IP` with the LogZilla server IP address or DNS name.

syslog-ng

Add the following to `/etc/syslog-ng/syslog-ng.conf`:

```
destination d_logzilla { udp("LOGZILLA_IP" port(514)); };
log { source(s_src); destination(d_logzilla); };
```

Restart syslog-ng: `systemctl restart syslog-ng`

rsyslog

Create a configuration file to forward all logs:

```
cat > /etc/rsyslog.d/50-logzilla.conf << 'EOF'
# Forward all logs to LogZilla
*.* @LOGZILLA_IP:514
EOF
systemctl restart rsyslog
```

For TCP transport, use `@@` instead of `@`:

```
*.* @@LOGZILLA_IP:514
```

Verification

Generate a test event and verify it appears in LogZilla:

```
logger -t sshd "Test message from Linux"
```

Incoming Log Format

Linux syslog messages follow the standard RFC 3164/5424 format:

```
<priority>timestamp hostname program[pid]: message
```

- **priority** - Facility and severity combined
- **timestamp** - Event timestamp
- **hostname** - Source host
- **program** - Process name (sshd, sudo, su, CRON, systemd)
- **pid** - Process ID
- **message** - Event-specific content

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Linux	Device vendor
Product	System	Device product
Event Class	auth	Event classification (auth, system)
User	jdoe	Username from authentication events
SrcIP	192.168.1.100	Source IP for SSH connections
Runas User	root	Target user for sudo/su/dzdo commands
Command	/bin/bash	Command executed via sudo or cron
Service	nginx.service	Systemd service name
Action	started	Systemd action (started, stopped, failed)
Auth Success	true	Authentication result
MitreId	T1110	MITRE ATT&CK technique ID
MITRE Tactic	Credential Access	MITRE ATT&CK tactic

Log Examples

SSH Failed Password

```
sshd[12345]: Failed password for invalid user admin from 192.168.1.100 port 54321
```

SSH Successful Login

```
sshd[12345]: Accepted publickey for jdoe from 192.168.1.100 port 54321 ssh2
```

Sudo Command

```
sudo: jdoe : TTY=pts/0 ; PWD=/home/jdoe ; USER=root ; COMMAND=/bin/bash
```

Su User Switch

```
su: Successful su for root by jdoe
```

Cron Job

```
CRON[67890]: (root) CMD (/usr/local/bin/backup.sh)
```

Systemd Service Started

```
systemd: Started nginx.service.
```

Systemd Service Failed

```
systemd: Failed to start mysql.service.
```

dzdo (Centrify) Privilege Escalation

```
adclient[2191]: INFO AUDIT_TRAIL|Centrify Suite|dzdo|1.0|0|dzdo
granted|5|user=jdoe(type:ad,jdoe@acme.com) pid=32224 status=GRANTED service=dzdo command=/bin/bash
runas=root role=ROLE_ADMIN
```

Dashboards

Dashboard	Description
Linux: Authentication	Auth events, failures, privilege escalation
Linux: System	Cron jobs, systemd services, system events

Triggers

Trigger	Description
`Linux: MITRE ATT&CK Threat Detected`	Any event with MITRE mapping
`Linux: SSH Authentication Failure`	SSH login failures (T1110)
`Linux: Sudo Privilege Escalation`	Successful sudo commands (T1548)
`Linux: Su User Switch`	Successful su commands (T1548)
`Linux: Su Authentication Failure`	Failed su attempts (T1110)
`Linux: dzdo Privilege Escalation`	Centrify dzdo granted (T1548)
`Linux: Service Failed`	Systemd service failures
`Linux: Authentication Event`	All auth class events
`Linux: System Event`	All system class events