LOGZILLA DOCUMENTATION

Postfix

LogZilla App Store application: Postfix

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/postfix

Overview

Postfix is a popular open-source Mail Transfer Agent (MTA) that routes and delivers electronic mail. Developed as a more secure and easier to administer alternative to Sendmail, Postfix is designed to be fast, easy to administer, and secure. It is widely used on Unix-like systems to route and deliver email.

App Function

- Parse Postfix syslog messages for delivery status and connection events
- Extract recipient/sender email addresses, relay servers, and client IPs
- Categorize events (delivery, delivery_failure, connection, reject, queue)
- Provide dashboards for monitoring mail flow and delivery issues
- Alert on bounced emails and relay access denials

Vendor Documentation

- Postfix Official Website (http://www.postfix.org/)
- Postfix Documentation (http://www.postfix.org/documentation.html)
- Postfix Basic Configuration (http://www.postfix.org/BASIC_CONFIGURATION_README.html)

Device Configuration

Postfix logs to syslog by default. Configure the syslog daemon to forward `mail` facility logs to LogZilla:

Edit `/etc/rsyslog.conf` or create `/etc/rsyslog.d/logzilla.conf`

Add a forwarding rule:

```
mail.*    @logzilla-server:514
```

Restart rsyslog:

```
systemctl restart rsyslog
```

Verification

Send a test email and verify events appear in LogZilla with program name `Postfix`.

Incoming Log Format

```
<date> <hostname> postfix/<service>[<pid>]: <queue_id>: <details> status=<status>
```

- **date** - Timestamp of the log entry
- **hostname** - Server generating the log
- **service** - Postfix component (smtp, smtpd, qmgr, local, bounce)
- **queue_id** - Unique message identifier
- **status** - Delivery status (sent, bounced, deferred, expired)

Parsed Metadata Fields

Field	Tag Name	Description
(auto)	`Event Class`	Cross-vendor classification (network or security)
Event type	`Postfix Event`	Event category (delivery, delivery_failure, etc.)
Status	`Postfix Status`	Delivery status (sent, bounced, deferred, etc.)
Recipient	`Postfix To`	Recipient email address
Sender	`Postfix From`	Sender email address
Relay	`Postfix Relay`	Relay server used for delivery
Client IP	`SrcIP`	Source IP from connection/reject events

Dashboards

Dashboard	Purpose
Postfix: Overview	Bounced/deferred/rejected counts, top failed recipients, relay servers

Triggers

Trigger	Condition	Actions
Postfix: Email bounced	status=bounced	mark_known, mark_actionable
Postfix: Email deferred	status=deferred	mark_known
Postfix: Relay access denied	reject event	mark_known, mark_actionable, notify

Log Examples

Successful Delivery

```
Jan  1 00:00:00 host1 postfix/smtp[1234]: 1234ABCD: to=<user@example.com>,
relay=smtp.example.com[192.168.1.1]:25, status=sent (250 OK)
```

Bounced Email

```
Feb 28 12:34:56 server-01 postfix/smtp[5678]: 9876ZYXW: to=<invalid@nowhere.com>, status=bounced
(User unknown)
```

Connection Event

```
Apr 10 08:15:30 mx1 postfix/smtpd[1111]: connect from mail.sender.com[10.0.0.50]
```

Relay Denied

```
May 20 14:22:45 mx1 postfix/smtpd[2222]: NOQUEUE: reject: RCPT from spammer.bad.com[192.168.100.99]:
554 5.7.1 Relay access denied
```