LOGZILLA DOCUMENTATION

Fail2Ban

LogZilla App Store application: Fail2Ban

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/fail2ban

Overview

Fail2ban is an intrusion prevention framework that protects servers from brute-force attacks. It monitors log files for failed authentication attempts and automatically bans offending IP addresses by updating firewall rules. Fail2ban supports SSH, Apache, Nginx, Postfix, and many other services.

App Function

- Parse Fail2ban syslog messages for ban/unban and detection events
- Extract banned IP addresses, jail names, and action types
- Categorize events (ban, unban, found, already_banned)
- Provide dashboards for monitoring intrusion prevention activity
- Alert on new bans and repeat offenders

Vendor Documentation

- Fail2ban Documentation (https://fail2ban.readthedocs.io/)
- Fail2ban GitHub Repository (https://github.com/fail2ban/fail2ban)

Device Configuration

Fail2ban logs to syslog by default. Configure syslog-ng to forward logs to LogZilla:

Edit `/etc/syslog-ng/syslog-ng.conf`

Add a destination and log statement:

```
destination d_logzilla { udp("logzilla-server" port(514)); };
log { source(s_src); destination(d_logzilla); };
```

Restart syslog-ng:

```
systemctl restart syslog-ng
```

rsyslog Alternative

For systems using rsyslog, add to `/etc/rsyslog.d/logzilla.conf`:

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

Verification

Trigger a ban (e.g., failed SSH attempts) and verify events appear in LogZilla with program name `Fail2ban`.

Incoming Log Format

```
<date>,<ms> fail2ban.<class> <level> [<jail>] <action> <ip>
```

- **date** - Timestamp of the log entry
- **class** - Fail2ban component (actions, filter, server, jail)
- **level** - Log level (NOTICE, INFO, WARNING, ERROR)
- **jail** - Jail name (sshd, apache-auth, etc.)
- **action** - Action taken (Ban, Unban, Found)
- **ip** - IP address being acted upon

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`Fail2ban`	Vendor name
`Product`	`Intrusion Prevention`	Product name
`Event Class`	`security`	Cross-vendor classification (security or system)
`MitreId`	`T1110`	MITRE ATT&CK technique ID (security events)
`MITRE Tactic`	`Credential Access`	MITRE ATT&CK tactic
`Fail2ban Class`	`actions`	Fail2ban component (actions, filter, server)
`Fail2ban Jail`	`sshd`	Jail name (sshd, apache-auth, etc.)

Tag Name	Example	Description
Fail2ban Action	ban	Action taken (ban, unban, found, already_banned)
SrcIP	192.168.1.100	Source IP address being banned/unbanned

Log Examples

Ban Event

```
2023-05-01 12:34:56,789 fail2ban.actions NOTICE [sshd] Ban 192.168.1.100
```

Unban Event

```
2023-05-01 12:45:00,123 fail2ban.actions NOTICE [sshd] Unban 192.168.1.100
```

Detection Event

```
2023-05-01 12:30:00,456 fail2ban.filter INFO [sshd]
Found 10.0.0.50 - 3 time(s)
```

Already Banned

```
2023-05-01 12:35:00,789 fail2ban.actions NOTICE [apache-auth]
iptables-multiport already banned 172.16.0.25
```

MITRE ATT&CK Mapping

Event Type	Technique	Tactic
Ban	T1110	Credential Access
Found	T1110	Credential Access

Event Type	Technique	Tactic
Already Banned	T1110	Credential Access

All security events indicate brute force attack detection (T1110). Unban events are administrative actions and do not receive MITRE mapping.

Dashboards

Dashboard	Description
Fail2ban: Overview	Bans, unbans, detections, repeat offenders, top banned IPs

Triggers

Trigger	Description
`Fail2ban: MITRE ATT&CK Threat Detected`	Events with MITRE technique mapping (T1110)
`Fail2ban: IP banned`	IP address banned
`Fail2ban: Repeated ban attempts`	IP already banned (persistent attacker)