LOGZILLA DOCUMENTATION

Receiving Events from Linux Bind

Route BIND DNS queries, responses, and server events to LogZilla by configuring named.conf logging channels and syslog-ng or rsyslog forwarding

Receiving Data in LogZilla · Generated April 29, 2026 · logzilla.ai/docs/receiving-data/linux-bind

Configure BIND DNS Logging

BIND (Berkeley Internet Name Domain) is the most widely used DNS server software. BIND logs DNS queries, responses, and server events to local syslog, which can then be forwarded to LogZilla via syslog-ng or rsyslog.

Prerequisites

- BIND DNS server installed and running on Linux
- Administrative access to the BIND server
- Syslog-ng or rsyslog installed for log forwarding
- Confirm syslog listener ports in LogZilla (see Syslog Settings (https://www.logzilla.ai/docs/administration/syslog-settings))
- Network connectivity between BIND server and LogZilla on syslog ports

Configure BIND logging

Modify `/etc/bind/named.conf.options` to enable syslog output:

```
logging {
    channel syslog {
        syslog local0;
        severity info;
        print-severity yes;
        print-category yes;
    };
    category lame-servers { null; };
    category default { syslog; };
    category queries { syslog; };
};
```

This configuration:

- Sends logs to syslog facility `local0`
- Includes severity and category information
- Logs DNS queries and general server events
- Discards lame-server notifications

Configure syslog-ng forwarding

Verify the main source exists in `/etc/syslog-ng/syslog-ng.conf`:

```
source s_src {
    system();
    internal();
};
```

Create `/etc/syslog-ng/conf.d/bind.conf` to forward BIND logs:

```
filter f_bind { facility(local0); };

destination d_logzilla {
    tcp("LOGZILLA_HOST" port(514));
};

log {
    source(s_src);
    filter(f_bind);
    destination(d_logzilla);
};
```

Replace `LOGZILLA_HOST` with the LogZilla server address.

Configure rsyslog forwarding (alternative)

For rsyslog, create `/etc/rsyslog.d/bind.conf`:

```
# Forward BIND logs (local0 facility) to LogZilla
local0.* @@LOGZILLA_HOST:514
```

Replace `LOGZILLA_HOST` with the LogZilla server address. The `@@` syntax uses TCP; use `@` for UDP.

Apply configuration

Restart the services to apply changes:

```
# Restart BIND
sudo systemctl restart named

# Restart syslog service (choose one)
sudo systemctl restart syslog-ng
# OR
sudo systemctl restart rsyslog
```

Verify in LogZilla

- Confirm reception by searching for events with facility `local0` or program containing DNS-related terms.
- Generate test DNS queries to produce log entries.
- For network-level troubleshooting, see Syslog Troubleshooting (https://www.logzilla.ai/docs/administration/syslog-troubleshooting).

Troubleshooting

- Verify BIND configuration syntax: `named-checkconf`
- Check service status: `systemctl status named syslog-ng`
- Test local syslog: `logger -p local0.info "BIND test message"`
- Monitor syslog files: `/var/log/syslog` or `/var/log/messages`

Related topics

- Syslog Settings (https://www.logzilla.ai/docs/administration/syslog-settings)
- Syslog Troubleshooting (https://www.logzilla.ai/docs/administration/syslog-troubleshooting)
- Syslog Relays (https://www.logzilla.ai/docs/administration/syslog-relays)