LOGZILLA DOCUMENTATION

Linux BIND

Adds rules, dashboards, and triggers for Linux BIND DNS server

LogZilla App Store · Generated June 14, 2026 · logzilla.ai/docs/logzilla-appstore/linux—bind

Overview

BIND (Berkeley Internet Name Domain) is the standard domain name service (DNS) software for Linux systems. It runs as a service daemon to provide DNS resolution services for networks.

App Function

- Parse BIND DNS query log messages
- Extract client IP, query domain, and record type
- Set `Vendor: Linux` and `Product: BIND` tags for filtering
- Provide dashboard for DNS query analysis
- Alert on zone transfer requests and potential amplification attacks

Vendor Documentation

- BIND 9 - Versatile, classic, complete name server software (https://www.isc.org/bind/)
- BIND (https://en.wikipedia.org/wiki/BIND)
- bind(2) - Linux manual page (https://man7.org/linux/man-pages/man2/bind.2.html)

Device Configuration

To enable query logging in BIND:

Edit the BIND configuration file (usually `/etc/named.conf` or `/etc/bind/named.conf`)
Add or modify the logging section to enable query logging
Configure syslog to forward logs to LogZilla
Restart the BIND service
Refer to the BIND documentation for detailed configuration options.

Incoming Log Format

The BIND query log format is comprised of space-separated fields in a fixed order. The query log entry first reports a client object identifier in `@0x` format. Next, it reports the client's IP address and port number, and the query name, class and type. It then reports whether the Recursion Desired flag was set (`+` if set, `-` if not set), if the query was signed (`S`), EDNS was in used along with the EDNS version number (`E(#)`), if TCP was used (`T`), if DO (DNSSEC Ok) was set (`D`), if CD (Checking Disabled) was set (`C`), if a

valid DNS Server COOKIE was received (`V`), or if a DNS COOKIE option without a valid Server COOKIE was present (`K`). After this the destination address the query was sent to is reported. Note: This reflects BIND `9.11.0` behavior.

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`Linux`	Vendor name
`Product`	`BIND`	Product name
`Event Class`	`network`	Cross-vendor event classification
`SrcIP`	`192.168.250.115`	Source IP address of DNS client
`Query`	`definitionupdates.microsoft.com`	DNS query domain name
`Query Type`	`A`	DNS record type (A, AAAA, MX, PTR, AXFR, etc.)

Log Examples

A Record Query

```
06-Jul-2022 11:12:04.202 client @0x7ff5b8000cd0 192.168.250.115#51530
(definitionupdates.microsoft.com): query: definitionupdates.microsoft.com IN A + (192.168.250.112)
```

AAAA Record Query

```
07-Jul-2022 11:15:38.170 client @0x7f026c008868 192.168.10.30#45166 (google.com): query: google.com
IN AAAA +E(0) (192.168.10.21)
```

Triggers

Trigger	Description
`BIND: DNS Error`	DNS errors (severity ≤ 3) - configuration or zone issues
`BIND: Zone Transfer Query`	AXFR/IXFR zone transfer requests - security monitoring
`BIND: ANY Query (Potential Amplification)`	ANY queries often used in DNS amplification attacks