LOGZILLA DOCUMENTATION

Linux dhcpd

Adds rules, dashboards, and triggers for Linux dhcpd

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

Overview

Linux dhcpd is a daemon that implements the Dynamic Host Configuration Protocol (DHCP) and the Internet Bootstrap Protocol (BOOTP). DHCP allows hosts on a TCP/IP network to request and be assigned IP addresses, and to discover information about the network to which they are attached.

App Function

- Parse DHCP message types (DHCPACK, DHCPREQUEST, DHCPNAK, etc.)
- Extract client IP, MAC address, hostname, and interface
- Set `Vendor: Linux` and `Product: dhcpd` tags for filtering
- Provide dashboard for DHCP lease monitoring
- Alert on DHCPNAK (lease denied) and error conditions

Vendor Documentation

- ISC DHCP 4.4 Manual Pages - dhcpd (https://kb.isc.org/docs/isc-dhcp-44-manual-pages-dhcpd)
- Arch Linux dhcpd (https://wiki.archlinux.org/title/dhcpd)
- Configuring a DHCP Server (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/networking_guide/sec-dhcp-configuring-server)

Log Source Details

Item	Value
Vendor	Linux distributions
Device Type	Linux OS
Supported Software Version(s)	dhcpd servers (tested on `isc-dhcp-server`)
Collection Method	Syslog
Configurable Log Output?	no
Log Source Type	Linux syslog

Item	Value
Exceptions	N/A

Incoming Log Format

dhcpd uses standard Linux syslog format. The message consists of a readable phrase explaining the DHCP operation, client device information, and IP addresses involved. There are no key-value pairs, delimited fields, or fixed-position fields.

Parsed Metadata Fields

The dhcpd app extracts client device type information from `DHCPACK` messages (DHCP IP address assignments). The message format is:

```
DHCPACK on <ip_addr> to <mac_addr> (<client_device_type>) via <interface>
```

Generated User Tags:

Tag Name	Example	Description
`Vendor`	`Linux`	Vendor name
`Product`	`dhcpd`	Product name
`Event Class`	`network`	Cross-vendor event classification
`DHCP Message Type`	`DHCPACK`	DHCP message type
`DHCP Client IP`	`192.168.254.100`	IP address assigned to client
`DHCP Client MAC`	`08:00:27:61:76:cd`	MAC address of client
`DHCP Client Hostname`	`VirtualBox`	Hostname of client device
`DHCP Interface`	`enp0s3`	Network interface serving request

Log Examples

DHCP IP Address Assignment

```
DHCPACK on 192.168.254.100 to 08:00:27:61:76:cd (VirtualBox) via enp0s3
```

DHCP Request

```
DHCPREQUEST for 192.168.254.100 from 08:00:27:61:76:cd (VirtualBox) via enp0s3
```

Triggers

Trigger	Description
`DHCP: Lease Denied (DHCPNAK)`	Lease denied - client misconfiguration or pool exhaustion
`DHCP: Error Event`	DHCP errors (severity ≤ 3) - pool exhaustion, config issues