LOGZILLA DOCUMENTATION

Dnsmasq

LogZilla App Store application: Dnsmasq

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

Overview

dnsmasq is a lightweight Linux daemon that provides DNS, DHCP, and TFTP services. It is commonly used in small networks and embedded systems. dnsmasq generates syslog messages for DHCP lease operations and DNS query activity, enabling network asset tracking and security monitoring.

App Function

- Parse dnsmasq DHCP messages (DHCPACK, DHCPREQUEST, DHCPDISCOVER, DHCPNAK, DHCPRELEASE)
- Parse dnsmasq DNS query logs
- Extract DHCP lease metadata (IP, hostname, MAC)
- Categorize DNS queries by type (A, AAAA, TXT, PTR, etc.)
- Flag TXT and ANY queries as security events (potential DNS tunneling)
- Provide dashboards for DHCP and DNS monitoring
- Alert on DHCP pool issues and suspicious DNS queries

Vendor Documentation

- dnsmasq Manual (https://thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html)
- Arch Linux dnsmasq Wiki (https://wiki.archlinux.org/title/dnsmasq)
- Debian dnsmasq Wiki (https://wiki.debian.org/dnsmasq)

Device Configuration

Configure dnsmasq to send logs to syslog, then forward syslog to LogZilla:

Edit `/etc/dnsmasq.conf` and ensure logging is enabled:

```
log-queries
log-dhcp
```

Restart dnsmasq:

```
sudo systemctl restart dnsmasq
```

Configure rsyslog or syslog-ng to forward dnsmasq logs to LogZilla.

Verification

Generate a DHCP request or DNS query, then verify events appear in LogZilla with the program name `dnsmasq` or `dnsmasq-dhcp`.

Incoming Log Format

DHCP Messages

```
DHCPACK(<interface>) <IP address> <MAC address> <hostname>
```

- **DHCP operation** - Message type (DHCPACK, DHCPREQUEST, DHCPDISCOVER, etc.)
- **interface** - Network interface name
- **IP address** - Assigned IPv4 address
- **MAC address** - Client hardware address
- **hostname** - Client hostname (if provided)

DNS Query Messages

```
query[<type>] <hostname> from <source_ip>
```

- **type** - DNS record type (A, AAAA, TXT, PTR, MX, etc.)
- **hostname** - Queried hostname
- **source_ip** - IP address of the DNS client

Parsed Metadata Fields

Tag Name	Example	Description
`Vendor`	`Linux`	Vendor name
`Product`	`dnsmasq`	Product name
`Event Class`	`network`	Cross-vendor classification (security for TXT/ANY)
`MitreId`	`T1071.004`	MITRE ATT&CK technique ID (TXT/ANY queries)

Tag Name	Example	Description
MITRE Tactic	Command and Control	MITRE ATT&CK tactic
DHCP Message Type	DHCPACK	DHCP message type
DHCP Assigned IP	192.168.1.100	IP address assigned to client
DHCP Assigned Hostname	workstation-01	Hostname of DHCP client
DNS Query Type	A	DNS query record type
DNS Query Hostname	www.example.com	Hostname being queried
DNS Query Source IP	192.168.1.50	IP address of DNS client

Log Examples

DHCP IP Address Assignment

```
DHCPACK(enp0s3) 192.168.254.101 08:00:55:66:77:88 dhcpnine
```

DHCP NAK (Pool Exhaustion)

```
DHCPNAK(eth0) 192.168.1.50 00:11:22:33:44:55 no address available
```

DNS Query

```
query[A] www.example.com from 192.168.1.50
```

DNS TXT Query (Security Event)

```
query[TXT] _dmarc.example.com from 192.168.1.50
```

MITRE ATT&CK Mapping

Event Type	Technique	Tactic
DNS TXT queries	T1071.004	Command and Control
DNS ANY queries	T1071.004	Command and Control

TXT and ANY queries are flagged as potential DNS tunneling or amplification attack indicators.

Dashboards

Dashboard	Description
DNSmasq: DHCP Overview	DHCP failures, new devices, lease activity
DNSmasq: DNS Overview	Query counts, security events, top clients

Triggers

Trigger	Description
`DNSmasq: MITRE ATT&CK Threat Detected`	Events with MITRE technique mapping (T1071.004)
`DNSmasq: DHCP Pool Issue (NAK)`	DHCP NAK indicates pool exhaustion
`DNSmasq: DNS TXT Query`	TXT queries may indicate DNS tunneling
`DNSmasq: DNS ANY Query`	ANY queries may indicate reconnaissance
`DNSmasq: Service Error`	Service-level errors (severity <= 3)