LOGZILLA DOCUMENTATION

# BlueCat DNS

Rule to parse BlueCat DNS DNSTAP telemetry and alert on threats

LogZilla App Store · Generated June 11, 2026 · logzilla.ai/docs/logzilla-appstore/bluecat-dns

## Overview

BlueCat DNS/DHCP Server (BDDS) is an enterprise DDI (DNS, DHCP, IPAM) appliance that provides authoritative and recursive DNS services. BDDS supports DNSTAP telemetry for real-time DNS transaction logging, delivering structured JSON records of all client queries, server responses, and recursive resolution activity.

## App Function

- Parse BlueCat DNSTAP telemetry events delivered as JSON via HTTP
- Extract DNS query metadata: domain names, query types, response codes
- Classify events by query type (standard network vs. security-relevant)
- Apply MITRE ATT&CK mappings for DNS-based threats (tunneling, recon)
- Provide dashboards for DNS traffic analysis and threat monitoring
- Alert on zone transfer attempts, DNS tunneling indicators, and service failures

## Vendor Documentation

- BlueCat DNS/DHCP Server Administration Guide (https://docs.bluecatnetworks.com/r/en-US/BlueCat-DNS-DHCP-Server-Administration-Guide)
- BlueCat DNSTAP Configuration (https://docs.bluecatnetworks.com/r/en-US/BlueCat-DNS-DHCP-Server-Administration-Guide/Configuring-DNS-data-collection-with-DNSTAP)
- DNSTAP Protocol Specification (https://dnstap.info/)

## Prerequisites

BlueCat BDDS must be configured to send DNSTAP telemetry to LogZilla via the HTTP receiver.

## Device Configuration

Log into the BlueCat Address Manager (BAM) web interface
Navigate to the BDDS server configuration
Enable DNSTAP data collection under **DNS > DNS Data Collection**
Configure the DNSTAP output to send JSON events to the LogZilla HTTP receiver endpoint:

- **URL**: `http://<logzilla-server>/incoming/raw`
- **Format**: JSON

- **Authentication**: LogZilla ingest token

Save and deploy the configuration

### Verification

After enabling DNSTAP, generate DNS queries against the BDDS server and verify events appear in LogZilla with `Vendor: BlueCat` and `Product: DNS` tags.

## Incoming Log Format

BlueCat DNSTAP events are structured JSON objects:

```
{
  "messageType": "<ClientQuery|ClientResponse|ResolverQuery|ResolverResponse>",
  "payloadType": "dnstap",
  "serverId": "<bdds-hostname>",
  "socketProtocol": "<UDP|TCP>",
  "sourceAddress": "<client-ip>",
  "requestData|responseData": {
    "question": [{"domainName": "<fqdn>", "questionType": "<A|AAAA|...>"}],
    "rcodeName": "<NoError|NXDomain|ServFail|Refused>",
    "answers": [{"rData": "<resolved-value>", "recordType": "<A|AAAA|...>"}]
  },
  "timestamp": "<ISO-8601>"
}
```

- **messageType** - Direction of DNS transaction
- **payloadType** - Always "dnstap" for this format
- **serverId** - BDDS appliance hostname
- **socketProtocol** - Transport protocol (UDP or TCP)
- **sourceAddress** - Client IP for client messages, 0.0.0.0 for resolver messages
- **requestData/responseData** - DNS question, answers, and response code
- **timestamp** - Event timestamp in ISO 8601 format

## Parsed Metadata Fields

| Tag Name | Example | Description |
|---|---|---|
| `Vendor` | `BlueCat` | Vendor identifier |

| Tag Name | Example | Description |
|---|---|---|
| Product | DNS | Product identifier |
| Event Class | Network | Event classification |
| Event Type | Threat | Event type (security events only) |
| SrcIP | 10.60.2.92 | Client IP making the DNS query |
| Domain | google.com | Queried domain name |
| BC Message Type | ClientQuery | DNSTAP message type |
| BC Query Type | A | DNS record type being queried |
| BC Response Code | NoError | DNS response code |
| Protocol | UDP | Transport protocol |
| MitreId | T1071.004 | MITRE ATT&CK technique ID |
| MITRE Tactic | Command and Control | MITRE ATT&CK tactic |

## High-Cardinality (HC) Tags

- SrcIP
- Domain

## Log Examples

### Client Query (A Record)

```
ClientQuery UDP google.com A NoError from 10.60.2.92
```

### Client Response (A Record)

```
ClientResponse UDP google.com A NoError from 10.60.2.92
```

### Resolver Query (Upstream Lookup)

```
ResolverQuery UDP azure.example.com A NoError
```

### NXDomain Response

```
ClientResponse UDP nonexistent.example.com A NXDomain from 10.60.2.39
```

### TXT Query (Potential DNS Tunneling)

```
ClientQuery UDP c2beacon.malware.example.com TXT NoError from 10.60.2.200
```

### Zone Transfer Attempt (AXFR)

```
ClientQuery TCP internal.corp.example.com AXFR NoError from 10.60.2.200
```

## Dashboards

The BlueCat DNS Overview dashboard provides:

- DNS event volume and rate monitoring
- Top queried domains and client IPs
- Query type and response code distribution
- Security event tracking (TXT/AXFR queries)
- NXDomain analysis for DGA detection
- Live event stream

## Triggers

| Trigger | Description |
|---|---|
| `BlueCat DNS: MITRE ATT&CK Threat Detected` | Any event with a MITRE technique ID |

| Trigger | Description |
| --- | --- |
| `BlueCat DNS: Potential DNS Tunneling` | TXT or NULL query types |
| `BlueCat DNS: Zone Transfer / Recon Query` | AXFR, IXFR, or ANY query types |
| `BlueCat DNS: DNS Service Failure` | ServFail response codes |
| `BlueCat DNS: Queries Refused` | Refused response codes |