PowerDNS dstore

Process. Distribute. **Analyze DNS Data.**

The Challenge

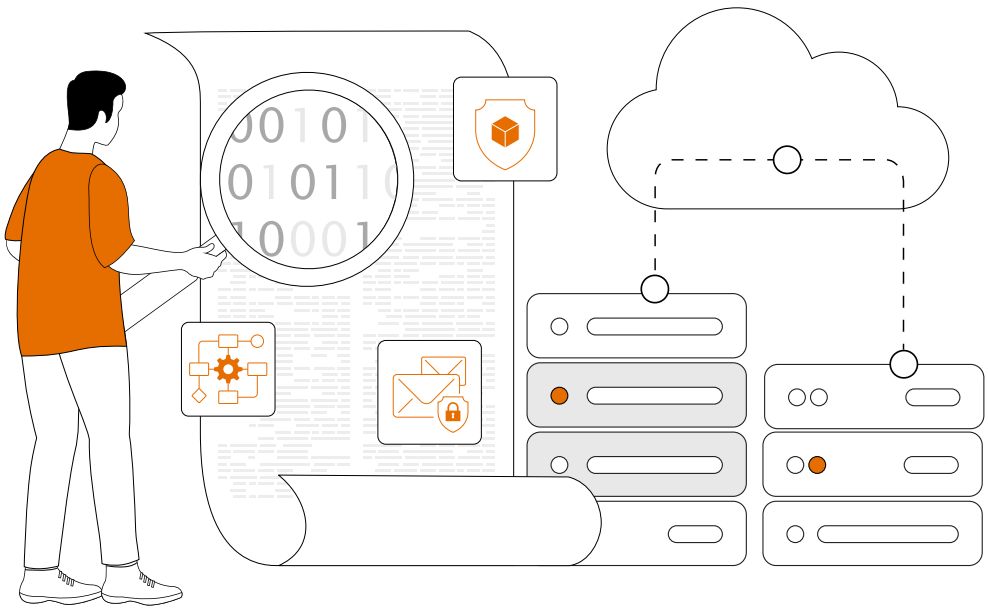
PowerDNS Recursor and DNSdist can generate detailed event data about DNS queries, responses, performance, and policy decisions. Turning this continuous stream of information into useful operational and security insights requires a reliable way to receive, filter, route, transform, aggregate, and retrieve the data.

DNS teams may need to build and maintain separate integrations for reporting, investigations, event storage, and downstream analytics systems.

The Solution

PowerDNS dstore is a modular platform for processing and distributing Protocol Buffer log messages generated by PowerDNS Recursor and DNSdist.

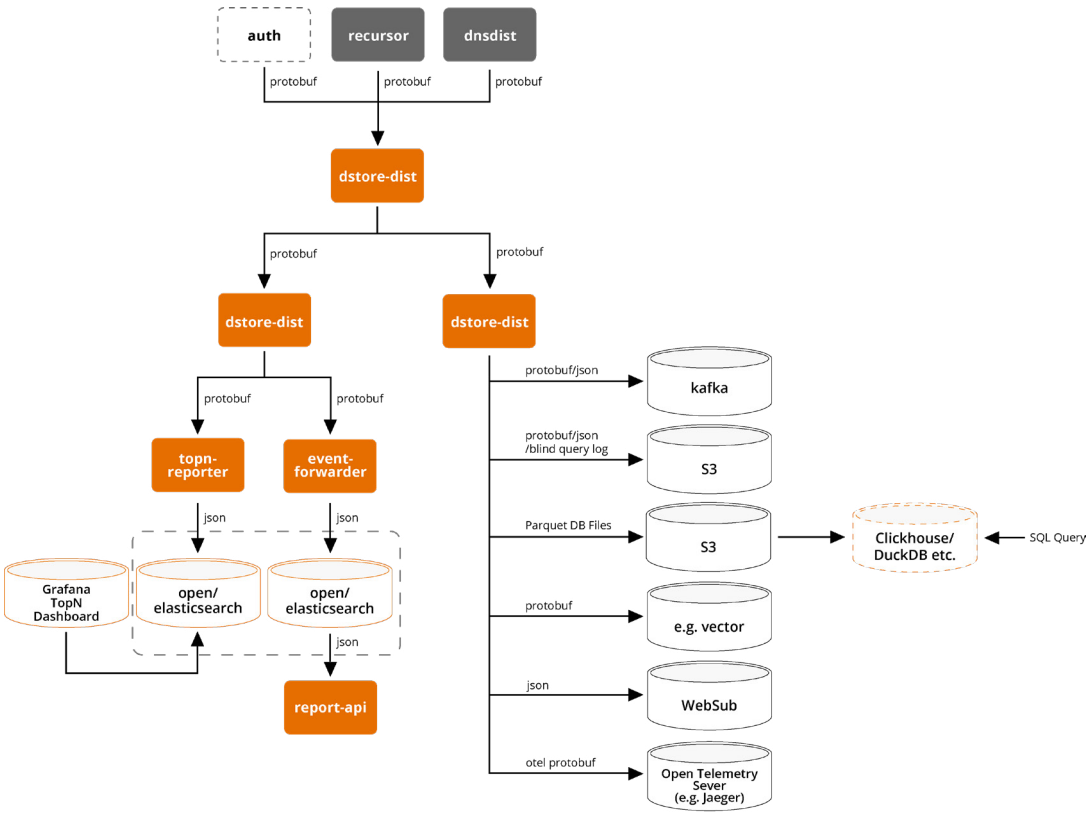
It receives DNS events over the network and can filter them, route them to multiple destinations, convert them into other formats, aggregate sampled data into reports, and store filtering-related events for later retrieval. This helps operators investigate DNS-related issues and gain insight into blocked or suspicious requests.



Key Capabilities

Modular Architecture
PowerDNS dstore consists of specialized components that can be combined according to the required processing and reporting workflow.

- **dstore-dist:** Receives, decodes, filters, transforms, and forwards protobuf events to configured destinations.
- **dstore-dist-top-reporter:** Aggregates protobuf events into reports, typically using sampled data, and stores the results in Elasticsearch or OpenSearch.
- **dstore-dist-eventforwarder:** Stores events related to DNS filtering in Elasticsearch or OpenSearch.
- **dstore-dist-report-api:** Provides an API for retrieving filtering-related reports and supports API-key-based authorization.
- **dnspcap2protobuf:** Converts DNS traffic from PCAP files into protobuf messages for subsequent processing by dstore.



Centralized DNS Event Processing
Receive structured protobuf events generated by PowerDNS Recursor and DNSdist using an extensible, language-neutral data format designed for efficient transport and processing. Events can represent DNS queries or combined query-and-response messages enriched with performance information.

Flexible Routing and Distribution
Use the dstore component dstore-dist to route incoming messages to one or multiple destinations. Each route can apply filters before forwarding the selected events, allowing DNS data to be directed according to operational requirements. Configuration is managed through a YAML-based configuration file.

Various Output Destinations
Forward DNS events to downstream systems or convert them into other supported formats and protocols, including Kafka. Destination types are available for PowerDNS protobuf, Kafka, storage, WebSub, and OpenTelemetry.

DNS Reporting and Top-N Analysis
Generate reports from protobuf events using dstore-dist-top-reporter. Data can be sampled before processing, helping produce reports such as overviews of the most frequently requested domains. Reports are stored in an Elasticsearch or OpenSearch backend.

Filtering Event Investigation
Store DNS filtering-related events with dstore-dist-eventforwarder and retrieve them through dstore-dist-report-api. This provides access to data that can support the analysis of blocked or suspicious DNS requests.

Detailed DNS Event Context
Protobuf messages provide structured context about DNS activity, including client and receiving IP addresses, transport protocol, timestamp, query name, query type, and query class. Depending on the event, messages can also contain response and performance information.

PCAP Conversion
Use the dnspcap2protobuf utility from the PowerDNS distribution to convert DNS traffic captured in PCAP files into protobuf messages that can be processed by dstore-dist.

Integrated Monitoring
All dstore components expose Prometheus metrics through a standard HTTP or HTTPS metrics endpoint. The metrics can be collected with Prometheus, visualized in tools such as Grafana, and used as the basis for alerting rules.

Key Benefits at a Glance

- Centralized DNS **event processing**
- Filtering **event investigation**
- **Modular deployment** architecture
- **Detailed** query and response **context**
- **Flexible** routing and filtering
- Kafka and analytics **integration**
- Multi-destination **data distribution**
- **Prometheus-based** monitoring
- DNS **activity reporting**

Ready to Turn DNS Events into Actionable Insights?

Discover how PowerDNS dstore helps you process, distribute, report on, and investigate DNS event data across your PowerDNS infrastructure.

Contact us

doc.powerdns.com