

# How to Improve DNS Resilience with Error Reporting

Willem Toorop <[willem@nlnetlabs.nl](mailto:willem@nlnetlabs.nl)>

Scott Hollenbeck <[sah@sahollenbeck.com](mailto:sah@sahollenbeck.com)>

Registration Operations Workshop (ROW) 15

29 September 2026

# The Problem: Resolution Errors, Operational Impacts

- Authoritative name servers can return results that create operational impacts for resolvers
  - Examples include DNSSEC-related errors, stale or forged answers, blocklist hits, etc.
- Resolvers traditionally have no way to alert name server operators to these issues beyond reliance on informal contacts within the DNS community
- Resolvers that can detect these issues and automatically alert name server operators to their existence can improve DNS resilience

# A Solution: DNS Error Reporting

- DNS Error Reporting, specified in RFC 9567, describes an in-band, automated method by which resolver operators can alert name server operators to many different error conditions

# Known Software Implementations

- Authoritative Name Servers

- BIND
  - <https://www.isc.org/download/>
- Knot DNS
  - <https://www.knot-dns.cz/docs/latest/singlehtml/index.html#dnserr-dns-error-reporting>
- NSD
  - From version 4.15.4 (expected mid October 2026)
  - <https://nlnetlabs.nl/projects/nsd/download/>

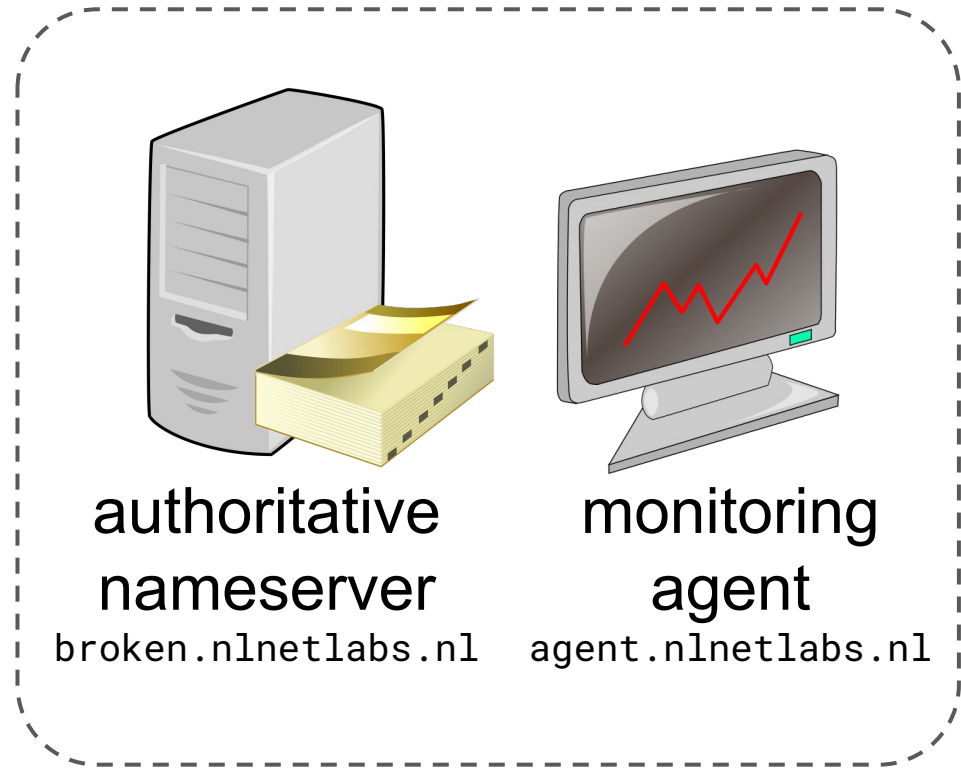
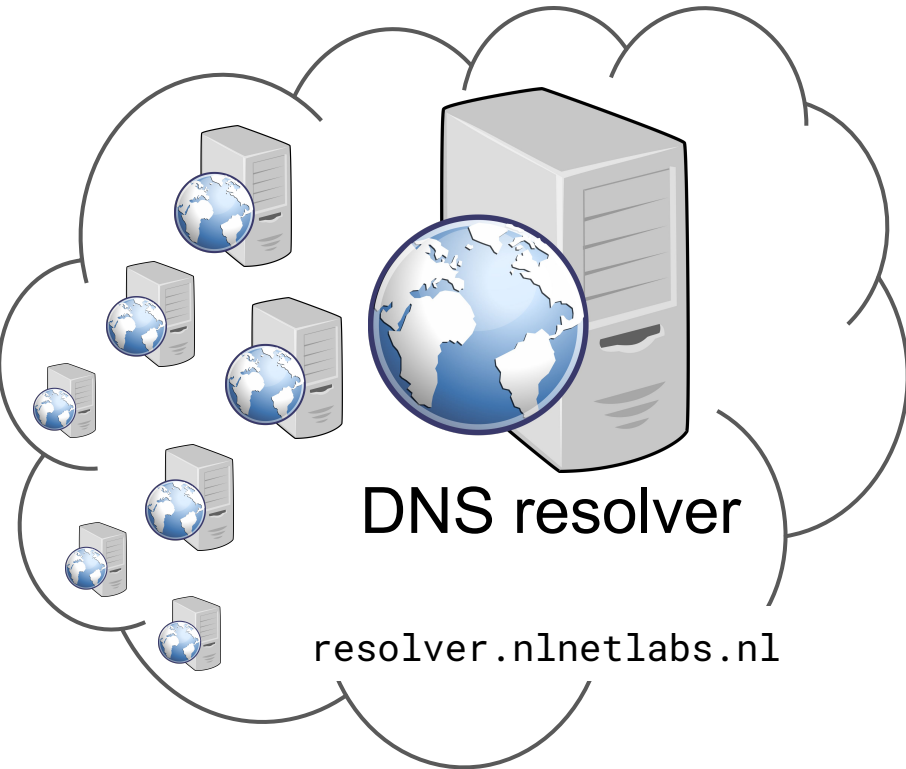
- Resolvers

- Unbound
  - <https://nlnetlabs.nl/projects/unbound/download/>

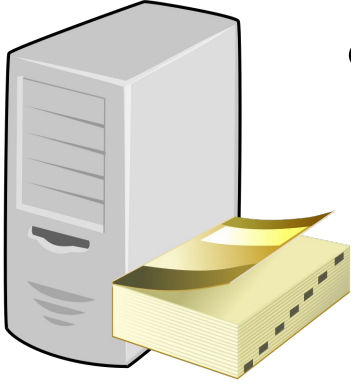
# Experimentation with DNS Error Reporting

- An informal effort was started in 2025 to explore interest in experimenting with DNS Error Reporting
  - Interest was confirmed
- NLnet Labs (Willem) deployed test servers
- SAHollenbeck (Scott) deployed monitoring agent add-ons
- Project status and experiment results are being discussed on the [“dns-resilience@dns-oarc.net”](mailto:dns-resilience@dns-oarc.net) mailing list

# Experimentation with DNS Error Reporting



# Experimentation with DNS Error Reporting



authoritative  
nameserver

broken.nlnetlabs.nl

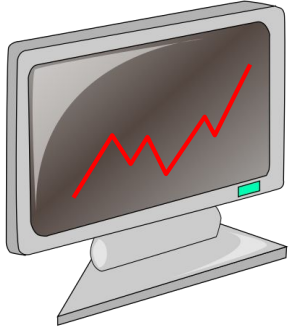
- BIND 9.21.21

```
zone "broken.nlnetlabs.nl" {  
    type primary;  
    file "broken.nlnetlabs.nl.signed";  
  
    send-report-channel "agent.nlnetlabs.nl";  
};
```

- Zone with on purpose broken RRs

- expired.nlnetlabs.nl (expired DNSSEC signatures)
- missing.nlnetlabs.nl (missing DNSSEC signature)
- invalid.nlnetlabs.nl (invalid DNSSEC signature)
- not-yet-valid.nlnetlabs.nl (signature valid in the future)

# Experimentation with DNS Error Reporting



monitoring  
agent

agent.nlnetlabs.nl

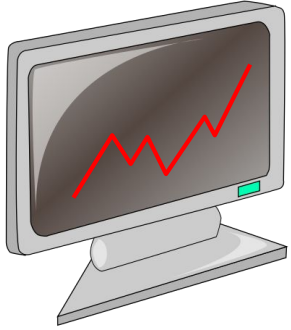
- BIND 9.21.21

```
zone "agent.nlnetlabs.nl" {  
    type primary;  
    file "agent.nlnetlabs.nl";  
    log-report-channel yes;  
};
```

- Zone:

```
$ORIGIN agent.nlnetlabs.nl.  
@      600  SOA   monitoring-agent.nlnetlabs.nl. (  
                                           sysadmin.nlnetlabs.nl. 1 0 0 0 600 )  
      600  NS    monitoring-agent.nlnetlabs.nl.  
3600   A    185.49.141.13  
3600   AAAA  2a04:b900:0:100::13  
  
*._er  600  TXT   "Thanks for the report"
```

# Experimentation with DNS Error Reporting



monitoring  
agent

agent.nlnetlabs.nl

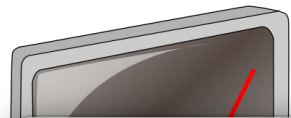
- BIND 9.21.21

```
logging {  
    category default { default_syslog; default_debug; };  
    category unmatched { null; };  
  
    category dns-reporting-agent { error_reporting; };  
  
    channel error_reporting {  
        file "dns-error-reporting/report.log" versions 30 size 25k;  
        print-time iso8601-utc;  
        severity info;  
    };  
};
```

- Log accessible over https

# Experimentation with DNS Error Reporting

- BIND 9.21.21



```
agent.nlnetlabs.nl/report.log x +
agent.nlnetlabs.nl/report.log
2025-08-21T13:31:54.370Z dns-reporting-agent '_er.1.servfail.nl.7._er.agent.nlnetlabs.nl/IN'
2025-08-22T14:25:21.020Z dns-reporting-agent '_er.16.expired.broken.nlnetlabs.nl.7._er.agent.nlnetlabs.nl/IN'
2025-08-22T14:25:48.556Z dns-reporting-agent '_er.16.missing.broken.nlnetlabs.nl.10._er.agent.nlnetlabs.nl/IN'
2025-08-22T14:28:10.595Z dns-reporting-agent '_er.16.missing.broken.nlnetlabs.nl.10._er.agent.nlnetlabs.nl/IN'
2025-08-22T14:28:25.733Z dns-reporting-agent '_er.16.invalid.broken.nlnetlabs.nl.6._er.agent.nlnetlabs.nl/IN'
2025-08-22T14:28:45.673Z dns-reporting-agent '_er.16.not-yet-valid.broken.nlnetlabs.nl.8._er.agent.nlnetlabs.nl/IN'
2025-08-22T14:28:56.041Z dns-reporting-agent '_er.16.expired-before-valid.broken.nlnetlabs.nl.8._er.agent.nlnetlabs.nl/IN'
2025-08-27T14:22:24.910Z dns-reporting-agent '_er.16.expired.broken.nlnetlabs.nl.7._er.agent.nlnetlabs.nl/IN'
2025-08-27T14:22:54.640Z dns-reporting-agent '_er.16.missing.broken.nlnetlabs.nl.10._er.agent.nlnetlabs.nl/IN'
2025-08-27T14:23:08.817Z dns-reporting-agent '_er.16.invalid.broken.nlnetlabs.nl.6._er.agent.nlnetlabs.nl/IN'
2025-08-27T14:23:24.870Z dns-reporting-agent '_er.16.not-yet-valid.broken.nlnetlabs.nl.8._er.agent.nlnetlabs.nl/IN'
2025-08-27T14:23:49.209Z dns-reporting-agent '_er.16.expired-before-valid.broken.nlnetlabs.nl.8._er.agent.nlnetlabs.nl/IN'
2025-08-28T19:57:17.733Z dns-reporting-agent '_er.16.expired.broken.nlnetlabs.nl.7._er.agent.nlnetlabs.nl/IN'
2025-08-29T06:49:38.437Z dns-reporting-agent '_er.16.expired.broken.nlnetlabs.nl.7._er.agent.nlnetlabs.nl/IN'
2025-10-08T12:29:26.818Z dns-reporting-agent '_er.1.invalid.broken.nlnetlabs.nl.7._er.agent.nlnetlabs.nl/IN'
2025-10-08T22:01:48.240Z dns-reporting-agent '_er.16.expired.broken.nlnetlabs.nl.7._er.agent.nlnetlabs.nl/IN'
2026-09-07T15:11:36.360Z dns-reporting-agent '_er.16.expired.broken.nlnetlabs.nl.7._er.agent.nlnetlabs.nl/IN'
```

# Experimentation with DNS Error Reporting



- Unbound 1.25.1

server:

`dns-error-reporting: yes` # Enable DNS error reporting

`ede: yes` # Not needed for DNS error reporting

`val-log-level: 2` # Additional text in Extended DNS Errors

DNS resolver

- Accessible over TCP, DoT, DoH and DoQ (but not UDP)

`resolver.nlnetlabs.nl`



user



resolver

*root*



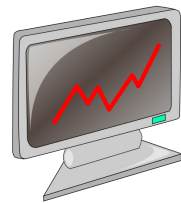
*nl*



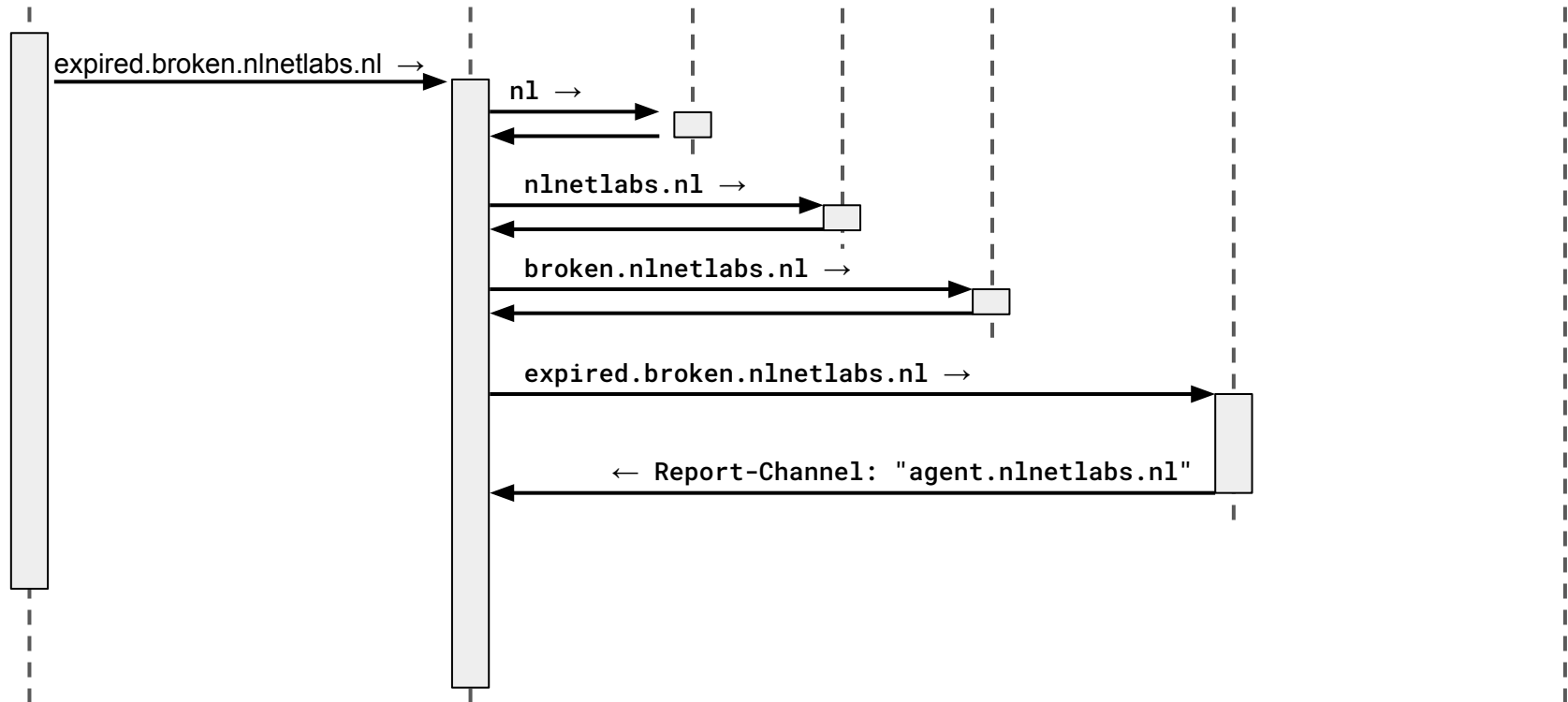
*nlnetlabs*



nameserver



agent





user



resolver

root



nl



nlnetlabs



nameserver



agent

expired.broken.nlnetlabs.nl →

nl

nlr

bro

exp

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58998
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; Report-Channel: "agent.nlnetlabs.nl"
;; QUESTION SECTION:
;expired.broken.nlnetlabs.nl. IN TXT

;; ANSWER SECTION:
expired.broken.nlnetlabs.nl. 3600 IN TXT "Signature Expired (7)"
expired.broken.nlnetlabs.nl. 3600 IN RRSIG TXT 13 4 3600 ...
```

← Report-Channel: "agent.nlnetlabs.nl"



user



resolver

*root*



*nl*



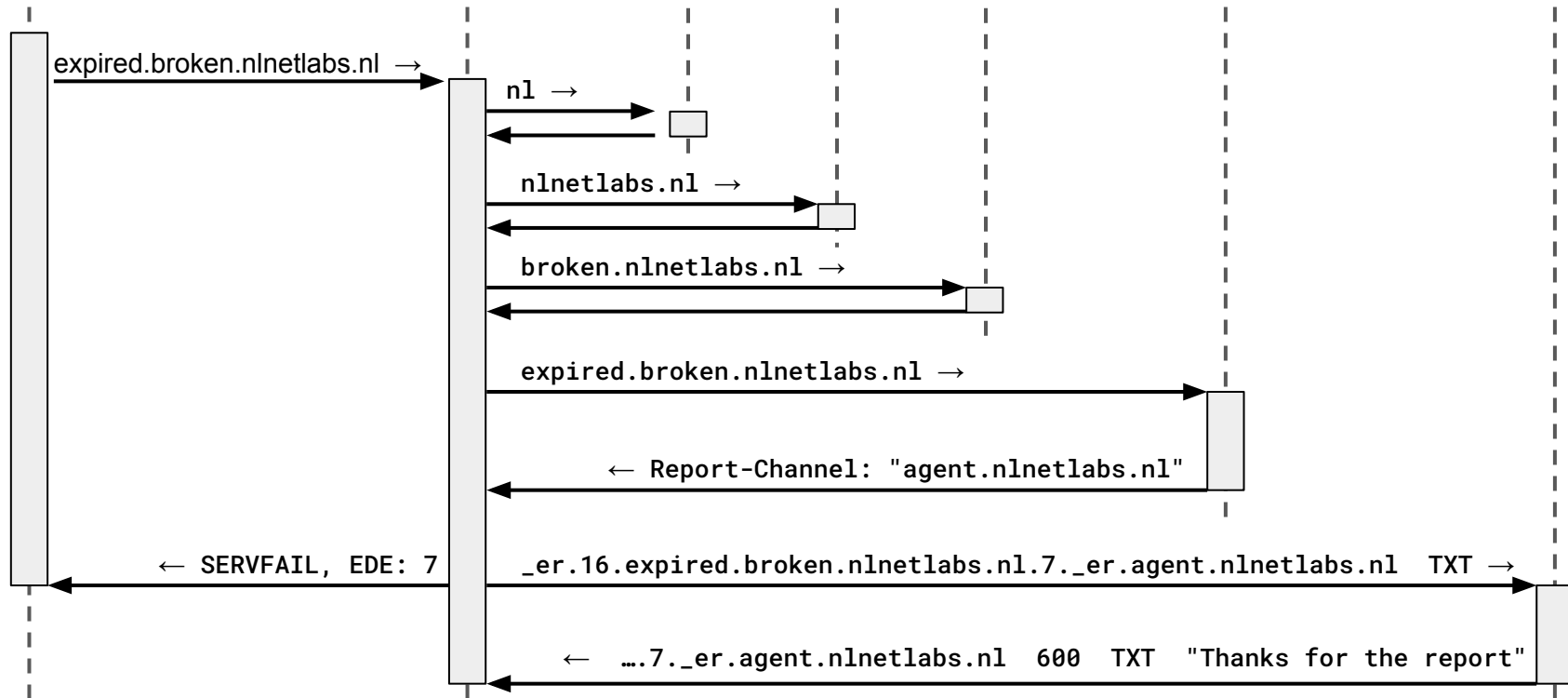
*nlnetlabs*



nameserver



agent





user



resolver

root



nl



nlnetlabs



nameserver



agent

expired.broken.nlnetlabs.nl →

nl →

nlnetlabs.nl →

```
;; opcode: QUERY, status: SERVFAIL
;; flags: qr rd ra; QUERY: 1, ANSWER: 0

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; EDE: 7 (Signature Expired): ...
;; QUESTION SECTION:
;expired.broken.nlnetlabs.nl. IN TXT
```

← SERVFAIL, EDE: 7

broken.

expired

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35426
;; flags: ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;_er.16.expired.broken.nlnetlabs.nl.7._er.agent.nlnetlabs.nl. TXT
;; QUERY SIZE: 88
```

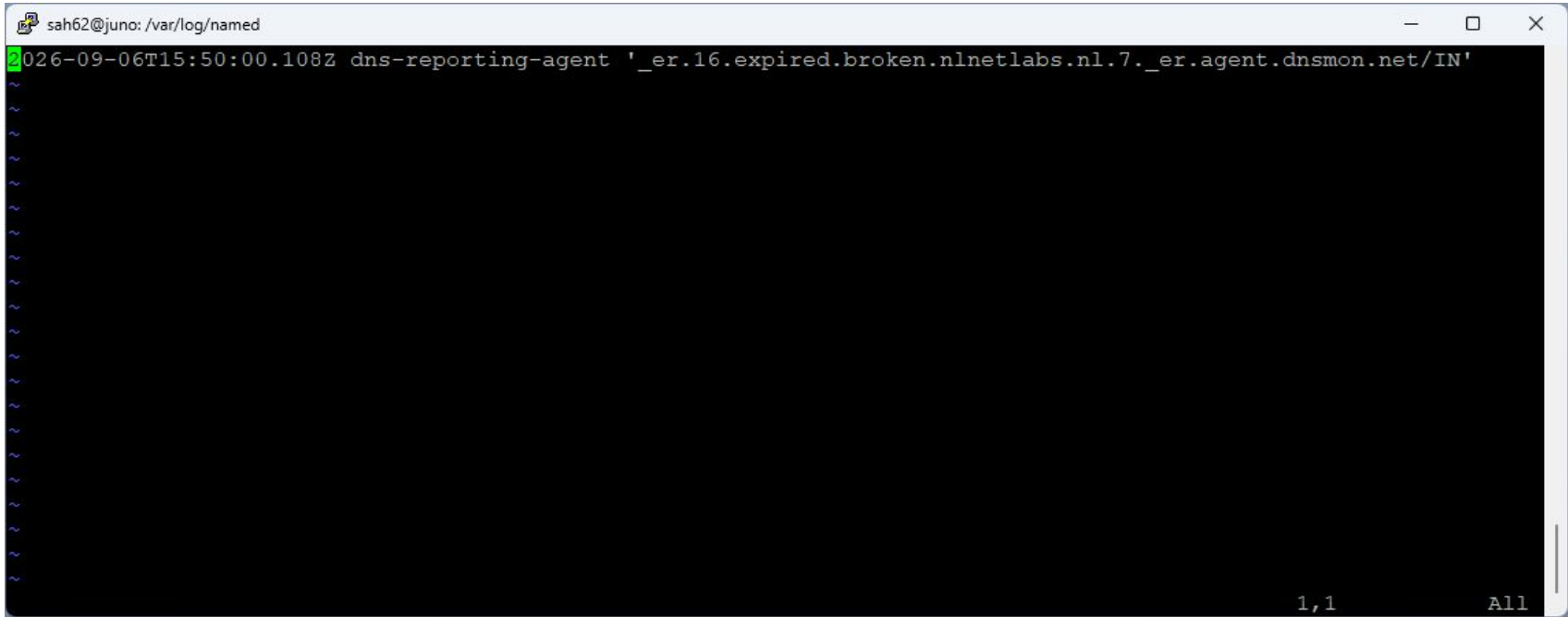
\_er.16.expired.broken.nlnetlabs.nl.7.\_er.agent.nlnetlabs.nl TXT →

← ...7.\_er.agent.nlnetlabs.nl 600 TXT "Thanks for the report"

# Making Error Reports Useful

- Error reports contain useful information
  - That information needs to be seen and acted upon by a human to be *truly* useful
- Authoritative name servers commonly log queries
  - Log entries are easily missed
- Additional tools are needed to process error reports when they're received
  - DNS authoritative name server software (we use BIND development release 9.21.25) that provides the monitoring agent service to capture the error reports
  - Software to process the monitoring agent log file (we use rsyslog)
  - Software to generate alerts in real time when a report is received (we use Graylog)
- Other solutions are possible depending on your operating environment
- *This is all beyond the scope of RFC 9567!*

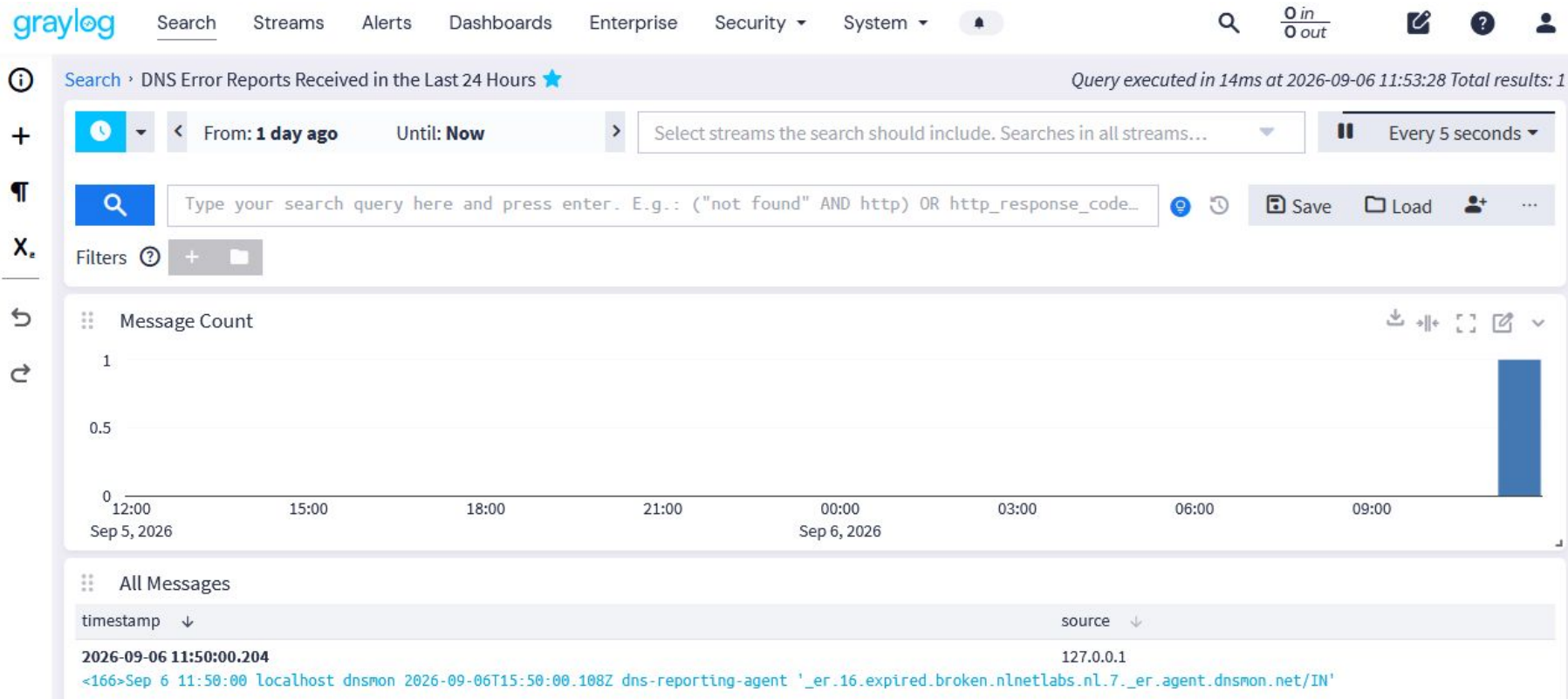
# Step 1: The Monitoring Agent Receives an Error Report



A terminal window titled 'sah62@juno: /var/log/named' displays a log entry. The entry is a single line of text: '2026-09-06T15:50:00.108Z dns-reporting-agent '\_er.16.expired.broken.nl.netlabs.nl.7.\_er.agent.dnsmon.net/IN''. The terminal has a black background with green text. The window title bar is light blue with standard minimize, maximize, and close buttons. The bottom right corner of the terminal shows '1,1' and 'All'.

```
sah62@juno: /var/log/named
2026-09-06T15:50:00.108Z dns-reporting-agent '_er.16.expired.broken.nl.netlabs.nl.7._er.agent.dnsmon.net/IN'
```

# Step 2: The Error Report is Detected



# Step 3: The Error Report is Processed and Alerted

Event notification: DNS Monitoring Error Report Received



sah@sahtollenbeck.com  
To sah6284@gmail.com

[Reply](#) [Reply All](#) [Forward](#) [...](#)

Sun 9/6/2026 11:53 AM

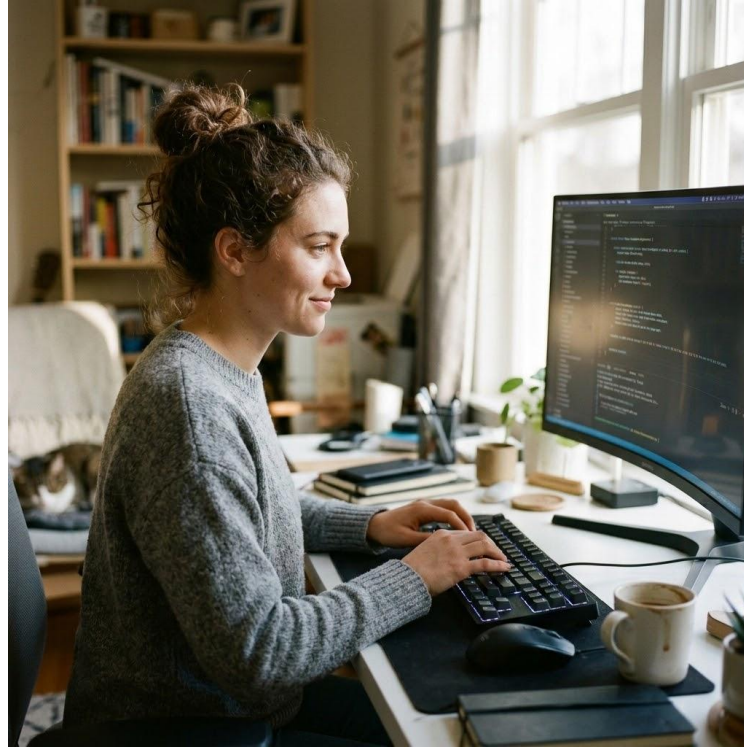
## Event Definition

|             |                                      |
|-------------|--------------------------------------|
| Title       | DNS Monitoring Error Report Received |
| Description | Custom event for DNS error reports.  |
| Type        | aggregation-v1                       |

## Event

|                      |                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alert Replay         | <a href="https://dnsmmon.net:9000/alerts/01M1VPSBA8S8YJNM41FWMB5BQ4/replay-search">https://dnsmmon.net:9000/alerts/01M1VPSBA8S8YJNM41FWMB5BQ4/replay-search</a> |
| Timestamp            | 2026-09-06T15:50:00.204Z                                                                                                                                        |
| Message              | DNS Monitoring Error Report Received                                                                                                                            |
| Source               | localhost                                                                                                                                                       |
| Key                  |                                                                                                                                                                 |
| Priority             | 3                                                                                                                                                               |
| Alert                | true                                                                                                                                                            |
| Timestamp Processing | 2026-09-06T15:50:00.204Z                                                                                                                                        |
| Timerange Start      |                                                                                                                                                                 |
| Timerange End        |                                                                                                                                                                 |
| Source Streams       | 00000000000000000000000000000001                                                                                                                                |

## Step 4: A Human Receives and Acts on the Error Report



# Other Resources

- rsyslog
  - <https://www.rsyslog.com/>
- Graylog
  - <https://graylog.org/downloads/>

# What Next?

- Additional operational experiments would be helpful!
  - We're aware of a few, but that's for those folks to talk about
- Security implications need to be explored further
  - Exposure of configuration mistakes, error reports are unauthenticated, etc.
  - Lots of detail in Section 9 of RFC 9567
- Operational implications need to be explored further
  - Volume of reports, bogus reports, etc. can overwhelm the human operator
  - Agent configuration options can help mitigate certain risks, but what are “best” practices?
- Subscribe to the mailing list
  - <https://lists.dns-oarc.net/mailman/listinfo/dns-resilience>
- Contact us for more information

The End!

**Thank you!**