DNSOP Working Group
Internet-Draft
Updates: 6195 (if approved)
Intended status: Standards Track
Expires: January 7, 2020

E. Hunt
D. Mahoney
ISC

July 6, 2019

A DNS Resource Record for Confidential Comments (NOTE RR) draft-hunt-note-rr-02

Abstract

While the DNS zone master file format has always allowed comments, there is no existing mechanism to preserve comments once the zone has been loaded into memory or converted to a binary representation. This note proposes a new RR type "NOTE", to be allocated from the Covert-RR type range proposed in [I-D.krecicki-dns-covert], so that confidential comments can be stored alongside zone data, and included in zone transfers when Covert semantics are supported by the secondary.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 7, 2020.

Copyright Notice

Table of Contents

1. Introduction

DNS zone master files may include comments: any text on a line following an unquoted semicolon is ignored when parsing the file [RFC1034]. These comments are often used by administrators to keep notes about the zone data; for example, the purpose of a particular host, or the person responsible for maintaining it.

When the zone is loaded, however, comments may be lost. Servers which dump backup copies of dynamically updated or automatically signed zones may obliterate comments that were in the original zone files. Secondary servers do not receive comment text when transferring zones from primary servers.

Comments could be stored in the zone itself as TXT RRs; these would be preserved after zone updates and across zone transfers. However, TXT records are available to any DNS query. Because zone file comments commonly include information about internal networks and/or personnel that could be of use to potential attackers, it is better for distribution of comment data to be restricted.

A Covert Resource Record, as described in [I-D.krecicki-dns-covert], could be used for the storage of private text information within zone data itself. This data could be transferred from primary to secondary servers when Covert semantics are supported, and but would be concealed from normal DNS queries (except from specific trusted DNS clients) and from secondary servers that do not signal their support of Covert data transfer.

This document proposes the allocation of a new RR type NOTE from the Covert-RR type range for this purpose. Comments that the operator wishes to be stored and transferred with zone data can be encoded as

NOTE records. Traditional zone file comments, indicated by semicolons, would still be ignored.

1.1. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. The NOTE RR Type

The NOTE RR is defined for all classes, with mnemonic NOTE and type code (TBD). The RDATA and presentation formats are identical to those of the TXT RR defined in [RFC1035], e.g:

```
$ORIGIN example.com.
joesbox   7200  IN  A       192.0.2.42
7200            IN  AAAA    2001:DB8:3F:B019::17
          0     IN  NOTE    "Desktop system for Joe Smith, x7889"
```

The RR type code MUST be allocated from the Covert-RR type range, and NOTE record data MUST be treated as Covert [I-D.krecicki-dns-covert].

3. IANA Considerations

IANA is requested to allocate a DNS RR type number from the Covert-RR type range for the NOTE RR type.

4. Security and Privacy Considerations

NOTE data should only be accessible via Covert DNS queries, because zone file comments commonly include information that could be of use to potential attackers. Failure to implement the restrictions outlined in [I-D.krecicki-dns-covert] could allow leakage of sensitive information.

5. Normative References

[I-D.krecicki-dns-covert]
Krecicki, W., Hunt, E., and D. Mahoney, "Domain Name System (DNS) Resource Record types for transferring covert information from primary to secondaries", draft-krecicki-dns-covert-00 (work in progress), July 2019.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Evan Hunt
ISC
950 Charter St
Redwood City, CA 94063
US

Email: each@isc.org

Dan Mahoney
ISC
950 Charter St
Redwood City, CA 94063
US

Email: dmahoney@isc.org