Workgroup: NTP
Internet-Draft: draft-ladd-nts-for-ntp-pool-00
Published: 28 February 2020
Intended Status: Informational
Expires: 31 August 2020
Authors: W. Ladd
Cloudflare

NTS for the NTP pool

Abstract

Network Time Security authenticates NTP servers. This document outlines an architecture that uses ACME and SRV records for the NTP pool to carry out NTS.

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 31 August 2020.

Table of Contents

1. Introduction

NTP is commonly provided via an NTP pool: a collection of servers behind a DNS load balanced and/or geolocated domain name. However Network Time Security requires certificates associated to the hostname of a server.

2. Conventions and 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.

The reader may wish to note that one of the two RFC references in the preceding paragraph was normative; the other was informative. These will be correctly identified as such in the References section below.

3. Background

The NTP pool uses dynamic DNS techniques to spread the load of NTP over a wide variety of servers. Unfortunately this creates challenges to the deployment of NTS: the servers all appear to share

the same hostname of the pool, and would all need certificates for that hostname.

To avoid these problems this draft presents a technique using SRV records and per-server hostnames along with ACME.

4. Clients

A client interested in using NTS with nts-pool.ntp.example.org will look up the SRV records for NTS-KE at nts-pool.ntp.example.org. This SRV record will point to Fully Qualified Domain names of the form servername.servers.pool.ntp.example.org, here called pool associated domain names.

Clients will then execute NTS-KE against the resolved IP address for those names, and continue as specified in [I-D.ietf-ntp-using-nts-for-ntp]

Clients SHOULD obtain multiple servers from a pool lookup and treat them as independent sources. If a source is unacceptable clients SHOULD replace them with new ones obtained from the pool.

Clients MAY periodically resolve the pool associated domain names to confirm the server is still trusted by the pool.

5. Pool Members

Pool members will register their servers and provide a servername, e.g. Alice. They will then use ACME with the HTTP-01 or ALPN challenge to obtain a certificate for alice.servers.pool.ntp.example.org.

6. Pool Operators

On registration of a server pool operators will create servername.servers.pool.ntp.example.org pointing to the provided IP address(s).

Once a certificate has been issued and NTS is confirmed operational, the pool may return SRV records pointing to the domain, either created by the pool or provided by the server operator.

Pool operators who remove a server from the pool MUST break the pool associated domain name. This prevents renewal of the associated certificate.

7. Security Considerations

This mechanism depends on the integrity of data in the DNS, for security and therefore DNSSEC should be used to protect the records.

Webservers on server in the pool MUST check the Hosts header of incoming HTTP requests to prevent cookie theft.

8. IANA Considerations

This document has no IANA actions.

9. Normative References

[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>.

[I-D.ietf-ntp-using-nts-for-ntp] Franke, D., Sibold, D., Teichel, K., Dansarie, M., and R. Sundblad, "Network Time Security for the Network Time Protocol", Work in Progress, Internet-Draft, draft-ietf-ntp-using-nts-for-ntp-22, 13 February 2020, <https://tools.ietf.org/html/draft-ietf-ntp-using-nts-for-ntp-22>.

10. Informative References

[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>.

Author's Address

Watson Ladd
Cloudflare

Email: watsonbladd@gmail.com