dnsop
Internet-Draft
Intended status: Informational
Expires: November 23, 2020

Y. Song
Y. Long
CFIEC-Guangzhou

May 22, 2020

DNS Authoritative server Management Based on Blockchain
draft-song-dnsop-dns-blockchain-00

Abstract

This document specifies a mechanism for managing authoritative server such as root server,thereby implement decentralized management of the authoritative server.Through distributed decision and distributed storage,encrypted inforamtion and records are stored adding the block to the blockchain.And the distributed authoritative servers share common blockchain which has detailed retrieval data for answering queries from the resolvers.

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 November 23, 2020.

Table of Contents

1. Introduction

The Domain Name System(DNS) is a simple query-response protocol,At present,DNS adopts centralized resolution system,that authoritative server is deployed by the independent entity and any modification requires the approval of the independent entity also.But there exists many risks for above-mentioned architecture,such as risk of disappearance, risk of blindness, risk of isolation,etc..Therefore,decentralized architecture for DNS is developing as a alternative option.

This document describes a new architecture for DNS,multiple authoritative servers in the same layer(e.g. root servers)as server nodes make up a node group.All server nodes in the same node group are peers,by which corresponding operations are governed together.And information and records stored in the server nodes can only be changed by reaching a consensus within the node group.Update from any server node can be automatically distributed to the other server nodes which provide redundant service for the data.Hence,there is no affect even though some server nodes are corrupted.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC8174].

1.2. Applicability

This document is applicable to authoritative server management,especially managing root server.A scheme to decentralize the architecture of authoritative server makes the trust from peer-to-peer to collective,thereby ensuring data consistency.

2. Authoritative server

As described in [RFC8499],authoritative server is a server that knows the content of a DNS zone from local knowledge,and thus can answer queries about that zone without needing to query other servers.

2.1. Root server

As described in [RSSAC026],root server is a particular anycast instance,as an authoritative server that answers queries for the contents of the root zone which contains all the information needed to find top-level domains.

2.2. Top-Level Domain Server

Top-level domain(TLD) server contains corresponding top-level domain zone that is one layer below the root server,such as "cn" or "com".TLDs are often divided into sub-groups such as country code top-level domains(ccTLDs),generic top-level domains(gTLDs).

2.3. Others

There are many other authoritative servers below the TLD server according to the actual condition.As one of the authoritative servers,there is nothing special from the point of view of the DNS,they are also used to find next-level domains or web servers.

3. Deployment of authoritative server

The DNS is a hierarchy,recursive resolver usually starts with root server when performing queries.Take root server as an example,root server stands at the top of the DNS hierarchy as shown in Figure 1.By requesting root server,related resource records of the TLD server can be found.Thus,the recursive resolver is referred to the specified TLD server to pursue the query.

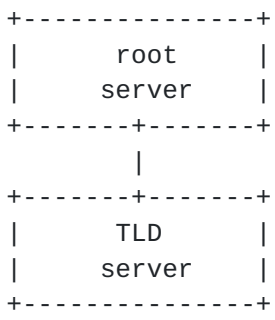

Figure 1: Architecture Between root and TLD

In the decentralized architecture as shown in Figure 2,root servers in the same layer make up a autonomous group,which can communicate with each other.Every root server in the autonomous group stores consistent data such as resource records through automatic synchronization. Meanwhile,above-mentioned root servers have peer administrative rights,that any update needs to be approved by all root servers.

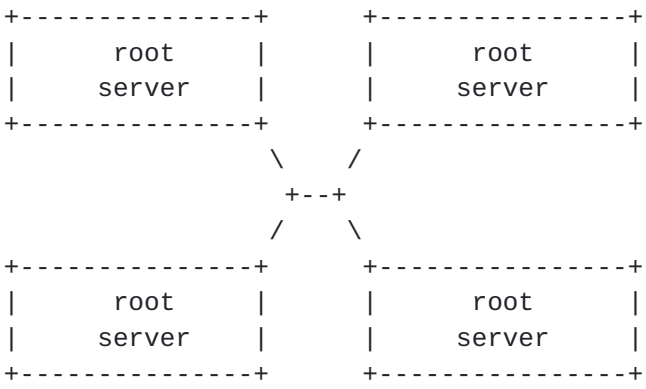

Figure 2: Architecture of the same layer Server

For autonomous group,it supports adding new server and removing expired server.About adding new server,every server in the autonomous group must make a descision by vote based on the identity of the newly added server within a valid time.On the other hand,the offline server can be removed from the autonomous group through a timeout mechanism.

4. Distributed Management

Authoritative server has zone which contains authoritative data organized into units.Root server,for example,has root zone which is used to refer the resolver to TLD server and let the resolver pursue the query.In order to keep the resource records about TLD server up to date,authoritative data needs to be constantly updated.And

underlying terms represent the distributed management for differnet types of update data.

4.1. Country Code Top-level Domains

For ccTLDs such as "cn",it is often governed by the specified nation.Therefore,when data about ccTLD is modified,update is submitted by the country-specific node server,and synchronized to all servers in the identical autonomous group.

4.2. Generic Top-level Domains

For gTLDs such as "com",it can be regarded as common management object.And any update about gTLD needs to be verified firstly using smart contract based on the modified constraint of protocol and format.After verification,a vote on whether to distribute update data to the servers in the autonomous group is triggered.Only through the approval of the servers in the identical autonomous group within a valid time,update data can be synchronized to all servers.

5. Features

- Autonomy
- Openness
- Equality
- Transparency

6. Security Considerations

The upadate information and records are stroed in the specific block based on blockchain,that corresponding information and records are encrypted by hashing and signing techniques,so that all information and records are immutable.

7. IANA Considerations

This document has no IANA actions.

8. 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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RSSAC026] Root Server System Advisory Committee(RSSAC), "RSSAC Lexicon", 2017, <https://www.icann.org/en/system/files/files/rssac-026-14mar17-en.pdf>.

Authors' Addresses

Yang Song
Guangzhou Root Chain International Network Research Institute Co., Ltd.
No.96 Qingsha Road, Dongchong Town, Guangzhou, Guangdong Province, China
Guangzhou 511458
P. R. China

Email: ysong@biigroup.cn

Yu Long
Guangzhou Root Chain International Network Research Institute Co., Ltd.
No.96 Qingsha Road, Dongchong Town, Guangzhou, Guangdong Province, China
Guangzhou 511458
P. R. China

Email: ylong@biigroup.cn