Workgroup: Domain Name System Operations
Internet-Draft: draft-yu-dnsops-disdm-04
Published: 20 June 2022
Intended Status: Informational
Expires: 22 December 2022
Authors:
H. Yu
Guangzhou Root Chain International Network Research Institute Co., Ltd.
D. Gong
Guangzhou Root Chain International Network Research Institute Co., Ltd.
Y. Song
Guangzhou Root Chain International Network Research Institute Co., Ltd.
Y. Liu
Guangzhou Root Chain International Network Research Institute Co., Ltd.

Multi Distribution master

Abstract

DM (Distribution Master) is used to transfer zone file data between the registry and the authoritative server. The centralized DM system has the risk of a single point of failure. The distributed DM architecture allows nodes to join and exit at any time to solve the single point of failure problem.

Requirements Language

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 22 December 2022.

Table of Contents

1. Introduction

Blockchain makes up for the shortcomings of the traditional DM system. The distributed feature improves the security of the system, the unlimited expansion feature improves the stability of the DM system, and the high autonomy feature brings the transparency of DNS data management. At the same time, the blockchain is the nemesis of DDoS attacks. Even if a certain node is attacked, other nodes can still operate normally without causing system breakdown. This draft is dedicated to building a distributed DM system and upgrading the traditional centralized DM node to a DM system without a central node. Using the existing blockchain technology, each node processes the domain file after reaching a consensus to ensure the uniformity and effectiveness of the domain file.

2. research status

In recent years, there have been few researches on DNS in foreign countries, and the main research is in the direction of architecture

and innovating on the architecture. The Russian National Nuclear Energy Research University proposed the main advantages and disadvantages of blockchain technology in the process of implementing a distributed DNS system, as well as the threats posed by blockchain . South Korea proposed a method to implement DNS using distributed ledger technology blockchain, and implement it using an Ethereum-based platform. In addition, a qualitative analysis and performance comparison evaluation of the existing domain name registration and domain name servers are carried out, and the security evaluation of the proposed system is carried out to improve the security problems of the existing DNS . The Institute of Electrical and Electronics Engineers puts forward a new blockchain-based decentralized DNS data storage method by studying the principles and characteristics of the blockchain, and implements a DNS decentralized system, establishes multiple parallel DNS nodes and storage areas The key information of file parsing data . Georgia State University proposes a system that can replace the current top DNS system and certification authority, providing higher scalability, security, and robustness. Based on distributed hash table, and using the domain name ownership system based on Bitcoin blockchain.

3. Multi-DM innovation

Multi-DM has the following two innovations: (1) Distributed DM system This project is dedicated to building a distributed DM system, upgrading the traditional centralized DM node to a DM system without a central node. Using the existing blockchain technology, each node processes the domain file after reaching a consensus to ensure the uniformity and effectiveness of the domain file. (2) Elastic contraction and expansion Traditional DM is a single node, which leads to excessive power of this node. If it is invaded or collapsed, it will paralyze the entire Internet. The nodes in the DM can withdraw or join at any time to ensure that the power of each node is consistent and dilute the power of the original single node.

4. Distributed multi-DM network management system

The distributed multi-DM network management system is the core of the architecture, and its responsibilities are as follows; (1) Load initial configuration, including DM static IP list, etc.;

(2) Use the election and heartbeat mechanism of the RAFT algorithm to elect the primary node, and initiate a heartbeat to other nodes through the primary node;

(3) Manage the joining and exit of DM. The joining of a new node requires that all nodes can recognize the node, and the exit needs

to notify each node to delete the corresponding information and the information stored by itself;

(4) Maintain the update of DM, including the change of node information in the system, etc.

Each DM runs on a P2P network, where the P2P network can ensure that each node can communicate, that is, two DMs can communicate at random, and the heartbeat mechanism is integrated on the P2P network. There is an IP list in each DM, which stores the IP information of all nodes in the system, and subsequent operations on the system are performed on this list. The addition of a new node means that the IP information of the new node is added to this list. When the node exits, the information about this node in this list is deleted. Node update means that the information of this node in this list is changed. The DM network management platform system has two states:

(1) Initialization state The initialization state is the process of establishing the network. Each node loads a static list. After the loading is completed, the IP of each node is recorded in each DM, and the primary node is elected. After the primary node election is completed, the state ends.

(2) Steady state After the election, it enters a stable state, and the primary node sends a heartbeat detection to the ordinary node to ensure the normal operation of each node. The joining, exiting and updating of new nodes are only allowed in a stable state. The joining of new nodes requires the approval of DMMC. The sign of joining is that the IP of the new node is added to the IP list of each node. When a node exits, it needs to completely delete its own information, while other nodes delete related information (identity verification information, IP information, etc.) of the node.

5. Node consensus technology

RAFT is a consensus algorithm. The so-called consensus is that multiple nodes reach a consensus on something, even in the case of partial node failures, network delays, and network partitions. Consensus algorithm is the core of blockchain technology, and in distributed systems, consensus algorithms are more used to improve the fault tolerance of the system, such as replication in distributed storage. The two main technical points of RAFT are problem decomposition and state simplification. Problem decomposition is to divide the complex problem of "node consistency in replication set" into several sub-problems that can be independently explained, understood, and solved. In RAFT, sub-problems include leader election, log replication, safety, and membership changes. The state simplification is better understood,

which is to make some restrictions on the algorithm, reduce the number of states that need to be considered, and make the algorithm clearer and less uncertain. PBFT provides (n-1)/3 fault tolerance on the premise of guaranteeing availability and safety (liveness and safety), which means that if there are n machines in the system, the maximum number of malicious/faulty nodes that the system can tolerate is (n-1)/3 pieces. (The malicious node may not respond or respond with wrong information). The distributed DM system uses a new algorithm combining RAFT and PBFT to solve the problem of trust and fault tolerance between nodes.

6. Threshold signatures

Threshold signatures introduce HSM, which is a system that provides a low-cost and high-security solution for key storage. For sensitive information such as keys, HSM provides logical and physical protection to prevent unauthorized access and intrusion. HSM provides tamper evidence (tamper evidence) and tamper resistance (tamper evidence) in two ways to prevent tampering. It is used in threshold signatures and is responsible for generating and storing the keys used to sign DNS zone files. The management of HSM is rotated by DMMC, and two HSMs are set up to achieve high availability of the system. HSM has the following functions:

Security key generation Security key storage and management Encrypt sensitive information Uninstall symmetric and asymmetric encryption calculations of the application server

The specific process is as follows: A. Leader node enters the signing status. B. Leader obtains the secret key from HSM, and generates the corresponding number of private key shares SKI according to the number of nodes. C. Leader will distribute the generated private key share to each node, and the node will reply the confirmation message after receiving it to ensure the success of distribution. D. Other nodes use private key shares to sign zone file data. E. After the node signs, the signed data is sent to the leader. F. When the Leader splits the private key shares according to the threshold, and the number is greater than the threshold value set, the signature is successful. G. Leader node sends the complete signature file to each node.

Each node uses the private key share to sign, and returns the digest with the signature to the HSM to form a complete signature, and the signature file is stored in the Primary node.

7. Security Considerations

8. IANA Considerations

This document does not include an IANA request.

9. Acknowledgements

The authors would like to acknowledge XXX for their valuable review and comments.

10. References

10.1. 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>.

[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>.

10.2. Informative References

[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>.

Authors' Addresses

Haisheng Yu
Guangzhou Root Chain International Network Research Institute Co., Ltd.
Xiangjiang International Technology Innovation Center, 41 Jinlong Road, Nansha District, Guangzhou
Guangzhou
China

Email: hsyu@biigroup.cn

Daobiao Gong
Guangzhou Root Chain International Network Research Institute Co., Ltd.
Xiangjiang International Technology Innovation Center, 41 Jinlong Road, Nansha District, Guangzhou
Guangzhou
China

Email: dbgong@biigroup.cn

Yang Song
Guangzhou Root Chain International Network Research Institute Co., Ltd.

Xiangjiang International Technology Innovation Center, 41 Jinlong Road, Nansha District, Guangzhou
Guangzhou
China

Email: ysong@biigroup.cn

Yan Liu
Guangzhou Root Chain International Network Research Institute Co., Ltd.
Xiangjiang International Technology Innovation Center, 41 Jinlong Road, Nansha District, Guangzhou
Guangzhou
China

Email: yliu@cfiec.net