International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-5)

Research Article | **May 2015**

Smart LDAP -based DNS Management System

Jitendra Kumawat*,
Department of Computer Science,
Amity University, Rajasthan, India

Shrinath Tailor
Department of Computer Science,
Pratap University, Jaipur, Rajasthan, India

Abstract—

This paper deals with the problem of managing DNS server management process. BIND software package is used for managing DNS data on a Unix based system. This is mainly done by editing ASCII files containing DNS zones, and then signaling the server process to reload them. This management process is prone to errors as it requires accessing the server over the actual or virtual console, thus it makes it unsuitable for complex operations in which related changes are required in several records and zones. The distributed system for DNS zone management is proposed by the authors. DNS served data are being stored in the LDAP-based directories. LDAP protocols are used by the DNS server in order to access its primary zones data. Management of DNS zones are done by the Web-based application. The advantages and disadvantages of the DNS server and the LDAP server are also discussed.

Keywords— ASCII, DIT, NIC, TCP

I. BACKGROUND TECHNOLOGY

The two most popular and important background technologies used in management system are :

- DNS
- LDAP

Domain Name System (DNS)

The Domain Name System (DNS) is a hierarchical naming system which is built on a distributed database for computers, any resource connected to the Internet or a private network. The DNS translates domain names meaningful to humans into numerical identifiers which are associated with networking order to locate and address these devices worldwide.
An analogy to explain the Domain Name System is that it behaves as the *phone book* for the Internet by translating human friendly computer hostnames into IP addresses. For example, the domain name *www.example.com* translates to the addresses *192.0.32.10* (IPv4) and *2620:0:2d0:200::10* (IPv6). The Domain Name System assigns domain names to groups of Internet resources and users in a well defined / meaningful way, independent of each and every entity's physical location. Because of this, World Wide Web (WWW) hyperlinks and Internet contact information remains consistent and constant even if there is a change in current Internet routing arrangements or the participant uses a mobile device. Internet domain names are easier to remember than IP addresses such as 208.77.188.166 (IPv4) or 2001:db8:1f70::999:de8:7648:6e8 (IPv6).The advantage of this is when the users recite meaningful Uniform Resource Locators (URLs) and e-mail addresses without having any knowledge of how the computer actually locates them.
The Domain Name System takes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers. The responsibility of each domain lies in the hands of their authoritative name servers and for their sub-domains other authoritative name servers are assigned. This mechanism makes the DNS distributed and fault tolerant and thus it helps to avoid the need of a single central register to be continually consulted and updated.

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an application protocol which is used for reading and editing directories over an IP network. Here directory means an organized set of records: for example, a telephone directory consists of an alphabetical list of persons and organizations with an address and phone number in each "record".
Directory is a hierarchical database with a number of distinguishing features:

- accessing of read and search directory is much more frequent than write;
- for accessing the directory there is a standard LDAP protocol;
- Standard directory schemes are used for describing format of the directory data.

Directory stores data in the forms of entries. a distinguished name (DN) is provided to Each entry for its identification. This distinguished name has a hierarchical form. The tree formed by Hierarchical entries is called directory information tree (DIT). An entry consists of attributes. There may be several values of each attribute. Attributes are defined by entry classes that must and may be present in the entry as well as formats of attribute values. The collection of related entry classes is called a directory scheme.

II. DNS SERVER

A DNS server is a computer registered to join the Domain Name System. It runs special-purpose networking software, provides a public IP address. It contains a database of network names and addresses for other Internet hosts.

DNS Root Servers

Private network protocols are used for communication of DNS servers with other servers. All DNS servers are form a hierarchal structure. Root servers are at the top level of the hierarchy, information regarding the complete database of Internet domain names and their corresponding IP addresses is stored in it. Overall 13 root servers are employed by Internet which are famous for their special role. For convenience, the servers are named as A, B, C and so on up to M. Ten of these servers reside in the United States, one in UK, one in Stockholm, Sweden and one in Japan.

DNS Server Hierarchy

The DNS is a distributed system i.e. only 13 root servers contain the complete details of domain names and IP addresses. At the lower levels of hierarchy, other DNS servers are installed and they contain only little information about database.
Businesses or Internet Service Providers (ISPs) owns the lower level DNS servers. For example, different DNS servers that manage the google.com, google.co.uk, and other domains are maintained by Google.
Networking of DNS is based on client / server architecture. User's Web browser acts as a DNS client (DNS *resolver*) and issues requests to Internet provider's DNS servers while navigating between various Web sites.
When a DNS server receives a request then it temporarily transforms from a server to a DNS client. The server then passes that request to other DNS server or to next higher level in the DNS hierarchy according to requirement. Finally, the request reaches at the server which has same matching name and same IP address in its database and the response is then sent back through the chain of DNS servers to the client.

WORKING of DNS

The Internet's fundamental building block is Domain Name System, or DNS. It is hierarchical, global and distributed host information database which is responsible for translating names into IP addresses and vice versa so that mail reach to its proper destination. One of the basic tasks of DNS is to find the corresponding IP address for a hostname or vice versa.
Steps included:
1) User's computer contacts the root level intrinsic name server to determine which primary name server contains user's Domain Name Records**.** Root level intrinsic name server is maintained by InterNIC.
2) After that root level internic name server returns the IP address of primary name server which is responsible for requesting the domain.
3) Next machine which is to be contacted by user's computer is the primary name server.
4) The primary name server holds IP address for the domain name in order to fulfill request made by user's computer.
5) At last, hosting server returns to web browser with the IP address.
6) With this IP address, the web browser is able to communicate with the company's web server and retrieve the requested web page

ADVANTAGES OF DNS

- It eliminates management of host tables.
- It is used on internet and internet cannot work without it.
- It is consistent on all hosts.
- It informs clients about the service addresses very easily.
- Transparency is achieved very easily

DISADVANTAGES OF DNS

- DNS query does not contain any information about the client who has triggered the name resolution.
- It provides no information about the topics included within the web page.
- A change is observed from the general legacy DNS.

III. LDAP SERVER

An LDAP session is started by client by connecting to an LDAP server known as a Directory System Agent (DSA), which is by default on TCP port 389. After that client sends request for an operation to the server and the server sends responses in return. The client then sends next request without waiting for the response to the previous request and after that the server sends the responses in any order.

- The client may request the following operations:
- Start TLS
- Search
- Compare
- Add a new entry
- Delete an entry
- Modify an entry

WORKING OF LDAP

LDAP directory service is based on a *client-server* model. One or more LDAP servers. The directory information tree (DIT) is made from the data present in one or more LDAP servers. The client then connects to servers and asks question from the server. The server provides answer to the client along with a pointer so that the client can get additional information. The Same view of the directory is seen by different LDAP servers. A name presented to one LDAP server is same at another LDAP server so it is not restricted to particular LDAP server. So, we can say that LDAP forms a global directory service.

ADVANTAGE OF LDAP NAMING SERVICE

- It provides us ability to consolidate information by introducing only application-specific databases in order to reduce the number of different databases which are to be managed.
- It allows more easy and fast data synchronization among masters and replicas.
- It is multi-vendor and multi-platform compatible.

DISADVANTAGES OF LDAP NAMING SERVICE

- It does not provide any support for pre-Solaris 8 clients.
- An LDAP server cannot be its own client.
- It is much more complex to set up and manage an LDAP naming service.

IV. CONCLUSION

Described LDAP-based DNS management system represents the solution for multi-server multi-administrator environment. Ideas for future development for this system include:

- Web-based management of the BIND configuration settings file;
- Web-based management of the BIND server process;
- Stronger LDAP authentication schemes (SASL);
- IPv6 support;
- DNSSEC support.

REFRENCES

[1]. V. Gupta, V. V. Lam, H. V. Ramasamy, W. H. Sanders, and S. Singh, "Dependability and Performance Evaluation of Intrusion-Tolerant Server Architectures," Proc. of the 1st Latin-American Symp. on Dependable Computing (LADC'03), LNCS 2847, Springer (2003) 81-101

[2] D. M. Nicol, W. H. Sanders, and Trivedi K. S., "Model-Based Evaluation: From Dependability to Security," IEEE Transactions on Dependable and Secure Computing, Vol. 1, (Jan.-March 2004) 48-65

[3] E. Malekian, Network Intrusion and Countermeasures, Nas Publications (2004) (in Persian)

[4] D. M. Nicol, S. W. Smith, M. Zhao, "Evaluation of Efficient Security for BGP Route Announcements using Parallel Simulation", Simulation Modeling Practice and Theory, Vol. 12 (2004) 187-216

[5] D. Nicol, S.W. Smith, "Modeling and Simulation in Security Evaluation", IEEE Security & Privacy(2005)

[6] Sahinoglu, M., Trustworthy Computing: Analytical and Quantitative Engineering Evaluation, Wiley-Interscience (2007)

[7] S. Porcarelli, F.D. Giandomenico, A. Bondavalli, and P. Lollini. "Model-Based Evaluation of a Radio Resource Management for Wireless Networks," Proc. of the Computing Frontiers, Ischia, Italy (April 2004)

[8] B. Littlewood, et al. "Towards Operational Measures of Computer Security," Journal of Computer Security, Vol. 2 (Oct 1993) 211-229.

