Indian J.Sci.Res. 17(2): 372-374, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

IMPROVING THE SECURITY IN CLOUD COMPUTING AND INTERNET OF THINGS APPLICATIONS

[1]B Ramana Reddy , Assistant Professor , Dept of CSE, Chaitanya Bharathi Institute of Technology
[2.] Dr. Madhu B K , Professor, Dept of ISE, R.R Institute of Technology,

Abstract— we introduce the concept of zoning in order to solve the problem of security and stability in Cloud Computing. We will have different zoning strategies from different perspectives. When we implement zoning at the switch fabric level, we can implement name server-based zoning and hardware enforced zoning. However, both of the implementations have their drawbacks. According to Brocade zoning implementations, we come up with the particular configuration methods called software zoning combining the advantages of both implementations.

Keywords- *storage area network; zoning; implementation*

I.INTRODUCTION

M ent, SAN become the preferred scheme in solving the problems such as bandwidth, capacity, and management. The security of SAN has caused concerns in the industry. Whether the storage architecture is secure or not influences the security of valuable data storage in SAN devices. So, we introduce zoning to control illegal access to fabric resources and avoid various attacks against SAN.

II. THE INFLUENCE OF ZONING ON STABILITY

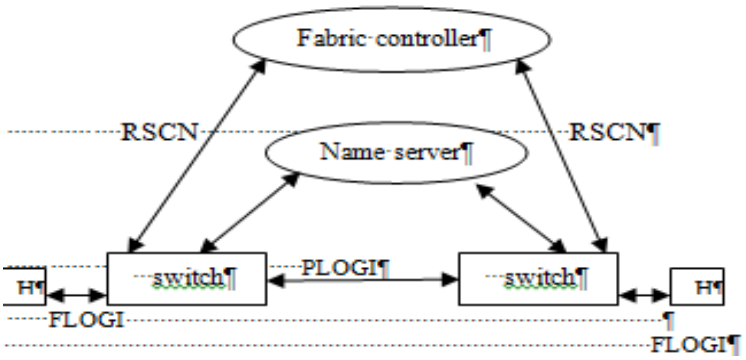
It's very important to maintain a stable network when networks become more complicated. First, we should learn about the basic procedure that devices login with the Fabric in SAN. Then we can analyze the traffic difference between zoning and no zoning.

A. Basic procedure that devices login with the Fabric

Devices such as servers and disks need to connect with F port in the fabric. First, device sends frame named FLOGI(fabric login) to the fabric. When the device receives the acceptance frame from the fabric, it continues to transmit PLOGI(port login) to the name server in the fabric in order to login and register its information with the name server such as its world wide port name and world wide node name (WWN). When the device receives the corresponding acceptance frame from the fabric, and if the devices need to

be aware of the topology of the fabric timely, it will transmit SCR (state change registration) frame to the fabric controller. In this way, the devices will receive RSCN (register state change notification) frame when the topology of the fabric have changed.

With the growth of mass data storage require



B. Traffic fluctuation analysis

In the absence of zoning, once a device connects to or removes from the fabric, the name server will send RSCN message to all the devices having registered SCR in the fabric. Then the devices having received RSCN will send query frames as shown in Figure 1 in the right. (When receiving GNN_FT frame, the switch returns a list of port ids and node names having registered support for the specified FC-4 type. When receiving GPN_ID frame, the switch returns the registered port name for the specified port id).In a large fabric, this can result in a significant amount of fabric service traffic in a short time, which goes against stability. Instead, if we have set zones, fabric controller will send RSCN message only in the same zone(s) with the abnormal device, which ensures a small traffic fluctuation in a small extent. As shown in Figure 2, we implement zoning in a fabric so that we can do tape backup in heterogeneous operating circumstances. HBA1 and DISK2 use the same OS, such as WindowsNT, HBA2 and DISK3 use another OS, such as Sun Solaris. In this zoning implementation, both HBA1 and HBA2 will share the content of tape library

[1]Corresponding Author

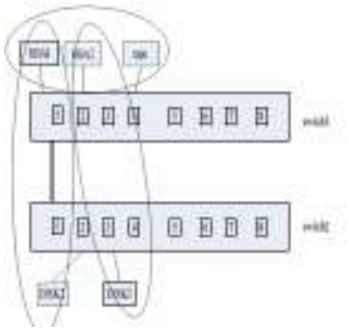


Figure 2. An implementation of zoning

III. THE STRATEGY OF ZONING IMPLEMENTATION

SAN zoning is like virtual LAN technology. According to different perspectives, there are host-based zoning, storage subsystem-based zoning and fabric zoning. Sometimes, we can use several zoning methods in a SAN and one device can belong to more zones. We only talk about fabric zoning as a mostly widely applied implementation in this paper.

A. Name Server-based Zoning

In the fabric name server records the WWN information of all the devices connected to the fabric. When host logins and sends GNN_FT frame and GPN_ID frame to get information about other devices as shown in Figure 3. After we have set zones, name server will send information about devices in the same zone(s).For example, in Figure 2 when HBA1 send query frame to the fabric, name server will look for the HBA1's WWN in WWN list and response the devices which are in the same zone with HBA1. So, the WWN of HBA1, HBA2, tape and DISK2 will be in the payload of response frame. Devices in other zones are invisible to the host such as DISK3. The advantage of name server-based zoning is its flexibility. When devices change their connected port, zone will not be changed. However, when an initiator has already known a target's address even if they are not in the same zone, the initiator can still access the target. Moreover, when we use name server-based zoning to control every approaching frame, it will add more delay in the switch software level. So, name server-based zoning scheme is the least recommended. But we could make use of the benefit of name server-based zoning to think about zoning problem.

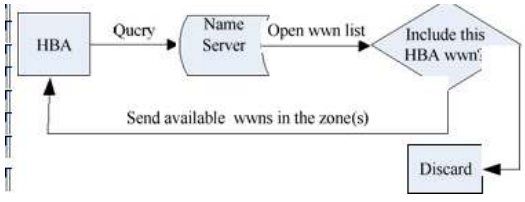


Figure 3. Name server-based zoning procedure

B. Hard Zoning

Hard zoning is hardware -based port allocation in the fabric. The basic principle is to maintain an access control table list in the hardware. When fabric receives a frame, it identifies forwarding port through examining frame's destination ID in the frame header. If the port number it entered and the forwarding port number are in the same zone, then the frame could be transmitted, otherwise it will be blocked. As shown in Figure 4, initiator connected to port 1 can't access target connected to port 5 because there is no route in the access control table list. We maintain port numbers in the access control table list. Port 1,6,7 are in the same zone; port 2,5,6 are in the same zone; port 3,6,8 are in the same zone; port 4,8 are in the same zone. Ports which are in the same zone can communicate with each other regardless of devices connected to the port. Comparing with name server -based zoning, hard zoning is more secure because if there is no link between two ports, then the security attacks from the networks will not success. In addition, hardware enforced strategy is much faster. However, hard zoning has its drawback. When you move the devices to another port in the fabric, the device may belong to another zone, and can't access the targets before. This will become hard to manage the whole network because you will not learn that which device is connected to which port. So, this zoning implementation is lack of flexibility.

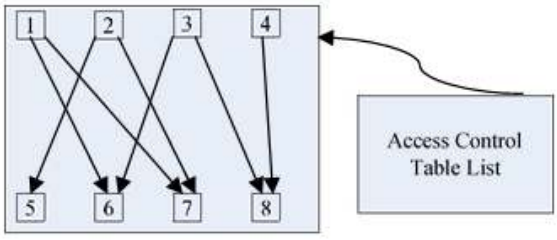


Figure 4. Hard zoning implementation

IV. *SOFT ZONING IMPLEMENTATION*

It is a recommended zoning strategy when we combine the advantages of the two zoning implementations. Zoning can be implemented in the ASIC chips. We can have more than one zoning configurations (make sure only one configuration active and others inactive in one time), and more than one zones in a configuration, and more than one members in a zone.

After studying Brocade zoning implementation, we come up with the zoning strategy below: we configure WWN based hard zoning. We can maintain WWN list of devices in the name server and then maintain the devices access control table list in hardware. All ISLs(inter switch link) within a hard zone are available to all the zones, providing load balancing for maximum data throughput under heavy workloads, as shown in Figure 2 the link between port 1 in switch 1and port 1 in switch 2. Then communication between devices conforms to the port

based hard zoning. Then when the devices become changed or shifted to a different port, the hardware below will identify the changes automatically and feed back to the application level as shown in Figure 6. Then we refresh create the new links immediately according to the Port IDs upper level supplies. In this way, the hardware configures access control table list dynamically in order to make zoning flexible and secure.

In this implementation, we add flexibility in the basis of security in the expense of hardware and software communication once the topology becomes changed. This can result in delay adding which is harmful to the switch. But, generally the topology will not change frequently and the networks will run in a relatively stable environment, then the most of time, the devices perform I/O with other devices in hard zoning.

wwn_HBA3	1,3
wwn_DISK1	2,1
wwn_DISK2	2,2
wwn_DISK3	2,3

Figure 5. Name server binding list

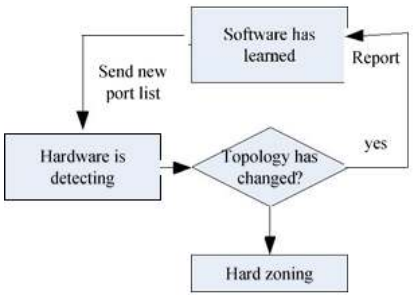


Figure 6. Procedure when topology changes

We take the communication between HBA2 and DISK3 in Figure 2 as an example. First, we create several zones manually according to our need. For example:Zone create “domain port ID”, “1,2;2,3;”That means port 2 in domain 1 and port 3 in domain 2 can communicate freely. There are basic links and ISLs between these ports. ISL configuration is invisable to user. In this circumstance,HBA2 and DISK3 can communicate in hard zoning complentation. Once we move DISK3 to port 5 in switch 2, the hardware is aware and notifies the upper level to change port zoning. The upper level configures new table list according to the new WWN information and binding port ID information in name server. Upper level notifies hardware to change table list according to the new list which it has transmitted. Then the link between port 1 and port 5 in switch 2 is created immediately. HBA2 and DISK3 begin to communicate freely again.

We select one principal switch to manage the entire the zones making use of the name server’s function that it can bind the device’s WWN with their port ID. Port IDs will be in the same zone if their WWNs are in the same zone. At last, the application level notifies the hardware to zoning configuration, and transmit all the zoning configuration information to all the switches in the fabric.

V.CONCLUSION

When data is growing dramatically, we choose the storage solution of using SAN. We can realize high-speed, easy-to-manage. We also need to make sure data resources are safe in SAN. Effective zoning in the fabric is beneficial to management in SAN. We hold two principles in zoning implementation: flexibility and security. Therefore we can use the WWN -based soft zoning. It can add flexibility.

REFERENCES

[1] Marc Farley. Building Storage Networks. McGraw-Hill Companies,2000, pp.201–205.

[2] Tom Clark. Designing Storage Area Networks: A Practical Reference for Implementing Fibre Channel and IP SANs,2/E. Addison Wesley Professional,2003, pp.62.

[3] ANSI INCITS 373. Fibre Channel Framing and Signaling (FC-FS). 2003,pp. 132–200.

[4] ANSI INCITS. Fibre Channel Generic Services-5(FC-GS-5). 2001, pp.135–276.

[5] ANSI INCITS . Fibre Channel Link Services(FC-LS).2006. 36-152

[6] Brocade SAN switch zoning. http://www.docin.com/p-10087202.html.2002.

[7] Brocade Guide to Understanding Zoning. Document number: 53-0000213-01. 2–4.

[8] Zoning implementation strategies for Brocade SAN fabric. www.brocade.com/san.2003,pp.3–8.

[9] Datalink.SAN Data Security & Fabric Management.2002,www.storagesearch.com.

[10] Joshua Staley, Suresh Muknahallipatna, Howard Johnson. Fibre Channel based Storage Area Network Modeling using OPNET for Large Fabric Simulations: Preliminary Work. 2007,pp.234-235.