A study of Storage Area Networksand issues in itsmanagement

Varsha Kulkarni[1],Dr. Nagaraj Bhat[2]

Electronics and Communication Dept.[1,2],R.V College of Engineering , Bangalore, India

mail.varshakulkarni@gmail.com[1],nbhat437@gmail.com[2]

Abstract: *A data centre has hundreds of servers and storage devices running on virtual machines that can be deployed and migrated over servers as per the requirement. If each server uses local storage, migration of this storage and restoration is mandatory. An attempt to organize and track storage throughout the data centre is quite tedious. Using a dedicated storage system like a storage array, it possible to collectively monitor and manage such a network. A storage area network is essentially a network dedicated to storage devices. A storage area network can interconnect devices in all its layers, therefore improving storage availability. Interconnecting all elements in SAN also reduces the chances of a single point of failure. Using the storage devices collectively improves their utilization. SAN offers to manage and maintain all devices in the network. Although SAN is beneficial, it has drawbacks when configuring, monitoring and managing components in a large-scale network. This paper consolidates the problems associated with SAN and offers possible solutions to overcome them.*

Keywords: Storage area networks ,Peer-zoning, Network Orchestration, Self-heal, Compliance check, Configuration

1. Introduction

A storage network is a computer network that provides access to block-level data storage. It consists of hardware and software. In a Storage area network (SAN) , a single server can manage and assign data-storage devices to multiple machines. Generally, as the data increases with an increase in computations, it becomes difficult to store. But, SAN overcomes this issue as SAN servers can handle multiple storage devices. Similar to a shared storage system, SAN allows direct access to the storage devices.[15]

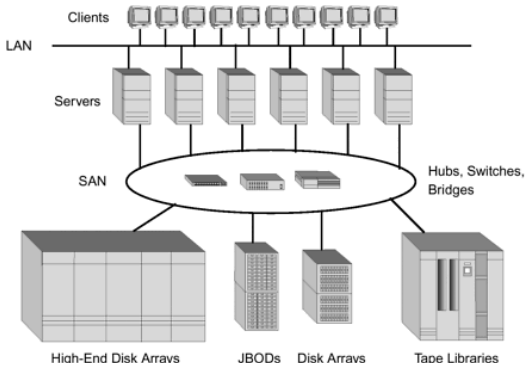

Figure 1. Storage Area Network

A typical SAN consists of 3 layers: host layer, fabric layer, and storage layer.[3]

1. Host Layer: The servers form the Host layer. Servers provide operating systems access to the storage area network using host adapters. The host layer can be connected to the storage layer directly or through a switch via the Host Bus Adapter.

2. Fabric Layer: Networking devices such as SAN switches, routers, gateway devices constitute the fabric layer. These devices move data between an HBA port of a server and the port of a storage device. SAN networks require redundancy and therefore consist of switches with redundant links. SAN switches connect the servers with the storage devices and are typically non-blocking, allowing data transmission across all attached wires simultaneously.

3. Storage layer: Data storage devices in a SAN form the storage layer. In SAN, RAID combines the storage devices, and it appears to unify the storage devices. Every storage device has a unique logical unit number. Servers or other storage devices in SAN can access storage devices using this number. It helps in restricting the access of different parts of the same SAN.

2. Storage Area Network Protocols

An The three layers communicate with each other with the help of network protocols. Unlike NAS that uses TCP/IP for communication and data transfer, SAN requires more distinct protocols. The two most common network protocols used by SAN are:

1. Fibre channel protocol: Fibre Channel Protocol (FCP) is the small computer systems interface protocol that utilizes an underlying Fibre Channel connection.[4] It connects storage elements to servers in Storage area networks. These standards define a high-speed data transfer mechanism to connect storage devices. FCP addresses the need for fast transfers of large blocks of data. It also provides a single standard for networking, storage and, data transfer. Fibre channel devices generally work with giga-bit technology.
2. iSCSI: Internet Small Computer Systems Interface is used to link data storage facilities using an Internet Protocol-based storage networking standard. SCSI commands are sent over IP networking. iSCSI can be applied to transmit data over LAN, WAN, or the global internet. It can enable location-independent data storage and data retrieval.[10]

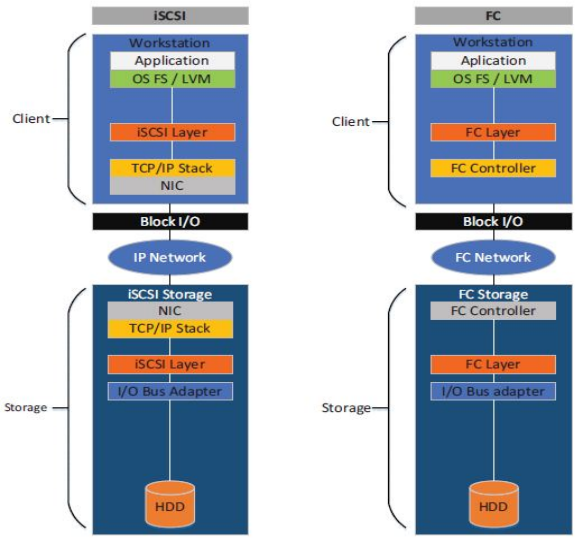

Figure 2. Layers of iSCSI and Fiber channel

As seen in figure 2, the overhead for FCP is much less when compared to iSCSI. When Random read and write and sequential read and write are implemented using both these

protocols, it is observed that FCP performs better than iSCSI due to the lesser overhead. For this experiment, a server and storage device are connected in two different paths. The first path has a Fibre Channel switch, and the second has an Ethernet switch.[1]

3. Zoning

It is essential to restrict the access of devices in the same SAN. This is achieved by making use of a Logic Unit Number that is assigned to storage devices. Only servers with the information of these unique identification numbers can access the storage resources. LUN masking is a method in which the HBA and software of server restrict accepting of the commands by LUNs. By preventing LUNs from command acceptance, these devices are masked. An alternate method to restrict access in SAN is by using fabric-controlled access or zoning.

Fibre Channel zoning is the method of partitioning the Fibre-channel fabric into subsets. Splitting it into subsets restricts the interference and enables management simplification. In zoning, each system in a SAN is allowed access to a controlled subset of devices existing in SAN. Zoning cannot be implemented in simple topologies of Fibre-channel and therefore only exists in switched fabric topology. There are two types of zoning: soft-zoning and hard-zoning.[11]

3.1 Peer zoning

To overcome the limitations of traditional zoning mechanisms, users have to create unnecessary zones. Doing this increases the complexity of zone configurations.[2] A new method known as peer zoning can enforce zones in FC. Peer zones are split based on zone names and consist of principal members and peer members. According to FC standards, there can be one or more principal members and peer members in a peer zone. Traditional zones and peer zones can exist in the same active zone set. Peer zoning allows communication only between a principal member and a peer member. Two peers in the same zone cannot communicate with each other. Switch management tools or any device with access to switch via the in-band protocol can configure Peer zones.

Peer zoning allows the configuration of one-to-many type zones, reducing the number of zones and ensuring optimal usage of switches. The hosts present in the peer zone cannot communicate with each other but can communicate with the target port. Therefore, disturbance at any host port is restricted only to that port and the target port. This shields unnecessary traffic from the remaining host ports.

4. Management Software

Along with a communication infrastructure, SAN also has a software management layer. The SAN software helps manage SAN elements. The software has to guarantee that data is moved directly between the storage devices without much server intervention. SAN software is usually installed on the servers, and the storage devices act as clients.[14]

There are two approaches for the SAN management software:

1. In-Band Management: There is a common network for the transmission of management data and storage data. Management data is between the storage device(client) and server.
2. Out-of-Band Management: The SAN software collects management data from the devices in the storage layer. The management data includes storage capacity bottlenecks, failure of storage devices.

It is possible to integrate the Simple Network Management Protocol(SNMP) with the management software.

5. Advantages and Disadvantages of SAN

Before considering SAN for the organization, it is important to assess its disadvantages

along with advantages.

5.1 Advantages

1. High performance: For high performance, the fabric used is Fibre Channel, though iSCSI is available as a fabric too. [1]
2. High scalability: As the requirement increases, new hosts and servers can be added to the network.
3. High availability: In a SAN deployment, there is no single point of failure as all elements are interconnected [9]. This ensures that there is an alternative path to maintain storage availability.
4. Advanced management features: SAN supports features like data encryption, storage replication, and self-healing technologies. These features are capable of maximizing the capacity of storage, increasing security. It also supports a data duplication feature required for backup.

5.2 Disadvantages

1. Complexity: SANs require their own configuration and management services. This makes SAN expensive. With an increase in complexity of the network, the cost increases making it difficult for organizations with low budgets.[3]
2. Scale: SANs on a smaller scale achieve satisfactory results but is not the same for more complex environments.
3. Management: Ensuring deployment of features such as self-healing, zoning, and LUN mapping is an important aspect of SAN configuration. As the complexity increases, management becomes problematic. Appropriate software is required to manage it efficiently.

6. Management issues in SAN

Even though SAN software makes the management of SAN quite simple, other issues arise due to manual error and a large network. The following are the management issues that arise in SAN.

1. Compatibility issues: The storage area network elements are generally manufactured by different vendors. For example, in a SAN, the switch could be from vendor1, storage device from vendor2. For smooth management of this network, the elements though from different vendors are required to be interoperable. All storage vendors provide a support matrix or a hardware compatibility list. If the devices from the two vendors previously mentioned are not compatible, communication cannot be established between the host layer and the storage layer.

2. Incorrect zoning: As the changes are made in zoning in SAN quite often, this can cause a host to lose access to the storage layer. Frequent changing of zones can also provide storage layer access to a host to whom it should not be provided. Zones generally contain 16-digit hexadecimal World Wide names that can cause manual error and zoning problems.

3. Exceeding the capacity limits: Saturating SAN ports cause bottlenecks which can transform into application problems. These application problems become difficult to diagnose. Determining if the port is 100% busy is easier compared to if the issue is with an overloaded inter-switch link.

4. Storage array configuration issues: During the configuration of SAN, LUNs are created and assigned to an HBA through a SAN port. Since LUNs are created manually, it is an intricate process prone to errors.

5. Host configuration issues : The hosts consist of an operating system, HBA- driver, hardware, firmware, multipathing software. All these components are to be configured according to the specifications given by the vendor. If not, they cause problems. Server virtualization increases the number of operating servers in a network. These virtual servers also require additional setup which can add to the original configuration issues.

6. SAN hardware failures: Although all the hardware is quite reliable now, the most common failure that can affect host access is SFP port failures, port card failures, and switch failures. An SFP port is a small form-factor pluggable port plugged into a switch. This port can fail due to rising temperatures caused by the speed of data entering or leaving the port. A switch can fail if its memory becomes full and has no space to process incoming data. It is necessary to monitor these changes and make assign appropriate tasks to counteract the problems.

7. Sluggish storage response times: Even after monitoring and configuring the SAN cautiously, storage devices can cause performance issues.

7. Network Orchestration

Network Orchestration is the process of programming the network behaviour automatically to ensure smooth coordination between the software and hardware elements in a network. The principle behind Network service orchestration is to separate network components from services and provide automatic configuration of the network as per the service specifications.
The principal goal of network orchestration is to minimize human intervention in processing network requests by automating them. Network Orchestration allows engineers to define gateways, routers, and security zones through configuration files or policies. These files are written in a programming language the control plane can understand. Network Orchestration automates tasks, such that setting up network services and deployment of the application can be at the same time rather than one after another. Some orchestrators are aware of the network and can analyse resource deployments based on the requirement. Orchestration also enables the network to be scaled based on user requirements making it both agile and responsive.

Network Orchestration can be applied in the following areas:

1. Establish overlays to dictate control and forwarding plane
2. Creation of different security domains in the network.
3. Ensuring workflows follow the right path by using traffic engineering
4. Provisioning various network services.
5. The direction of the workflow and management of that information.
6. Automation of interface or routing configuration using IP or OpenFlow protocol.

Orchestration can also manage the creation, upgrade, and operation of containers deployed in the network. It can also manage the connection between multiple containers to create a more comprehensive application. Containers generally are a set of programs of microservices corresponding to a service offered in the network management.

8. Solutions to Management issues

8.1 Automatic Configuration

The Orchestrator can provide a user interface with elements present in the network. Including configuring, monitoring services in the software reduces the probability of device configuration error. Since the software can provide a wholesome view of the network, it becomes easy to determine which devices are causing the network to fail.[12]

8.2 Naming security domains

Despite the advantages of peer zoning, the zones must still be configured manually using a switch CLI or GUI. Automating this process of configuration is called target-driven peer zoning(TDPZ). Implementing TDPZ, zones do not require any pre-configuration before the provisioning of hosts. Without TDPZ, it is required that the zones be configured before host and LUN configuration on the target side. Using TDPZ enables users to display and read zones from the storage array without the need to use another management tool. This eliminates any errors during the configuration of security domains. The Orchestrator can incorporate templates for each type of device in the network. These templates can be programmed to enable or disable TDPZ for a particular device.

8.3 Self-healing

Some devices in SAN require periodic monitoring and correction to work efficiently. [5] introduces the concept of self-heal with a layer-2 topology discovery mechanism. The control plane needs to ensure its reliability after the topology discovery. The authors propose a technique of self-heal to boost the resilience of the control plane without compromising the performance. The Self-healing topology discovery protocol can discover and maintain an accurate network view. It optimizes the reliability and discovery of the current service. To increase the robustness of the control plane, it combines a self-healing attribute along with the layer-2 topology discovery mechanism. The Automatic Fault Recovery mechanism is the self-healing attribute consisting of two elements: Autonomic manager and managed components. The autonomic manager monitors the "managed components." It also analyses the data collected and optimizes the performance of the network. Each "managed component" consists of sensors to track the states of the neighbouring links.
The managed component performs pre-determined steps when the network detects a failure of a port. [7] introduces a self-healing router architecture. Generally, self-healing router architecture requires the use of redundant routers. The redundancy causes area overhead. This paper proposes a method of self-healing without redundancy by providing flexibility to repair 50% of the routers without the use of spare routers.

If an orchestrator is developed with self-healing capability it can monitor the environment and act automatically depending on the conditions. It can identify states of physical ports for failure impact assessment, root cause analysis.
For example, consider an SFP port. The data rate varies from high megabits to gigabits. There is a change in the temperature of the port depending on the rate at which data is transferred. A persisting high temperature at the port can damage the hardware and result in transmission failure. To prevent this, self-healing is required. It can be monitored as follows: When the temperature reaches the threshold, reduction in the transfer speed to megabits until it cools down.
Another example of self-healing could be in a switch. A switch contains the data of the forwarding plane. The switch also stores a backup of this data to avoid problems if there is a failure. Over time, the backup data consumes the switch memory, causing problems while storing new forwarding data. By using self-heal, the orchestrator can monitor the memory and can clear the backup data.

Self-healing can solve the capacity saturation problem discusses previously.

8.3 Compliance check

All the devices present in a network are from different vendors. Therefore, for the devices to stay connected and communicate without errors, they must be compatible. Every device manufacturer provides a compatibility matrix indicating the device versions compatible with another device. By incorporating periodic checks in the orchestrator, the compatibility of all devices can be verified. The Network orchestration software can also be given permissions to upgrade devices automatically[13] or manually to maintain connectivity in the network.

8.4 Storage devices

The type of storage device used in the network plays an important role in determining the response time of the network. A significant difference is observed in performance when the storage device is a Solid-State drive and when it is a hard drive. An SSD provides better performance in access times, request time, and reliability[8].

9. Conclusion

Storage Area Networking is preferred for large data centres with many network elements and storage devices. All elements in a SAN are interconnected and therefore, eliminate single-point of failure. SAN has a software layer apart from the three existing layers. Despite that, management of such a network is difficult due to incompatibility of devices, error during host configuration, error during zone configuration, choice of storage device, hardware failures in the network. If a Network Orchestrator incorporates the features discussed above, the automation of SAN management improves drastically. The self-healing technology minimizes the time for diagnostics and ensures the longevity of the device in the network.

10. Future Scope

The software can also include application-based containers to run various services. These microservices can provide the user with the options to enable automatic log out, set buffer allocation percentage, and control the speed at ports. By using the right containers and microservices, the software can also provide the user with an option of flow control and the ability to vary the Maximum Transfer Unit.

11. References

11. 1Journal Article

[1] M. Kojić, B. Đordević, V. Timćenko and S. Štrbac, "Storage performance analysis of iSCSI and Fibre Channel protocol," 2019 27th Telecommunications Forum (TELFOR), 2019, pp. 1-4, doi: 10.1109/TELFOR48224.2019.8971162.

[2] Rupin Mohan HPE, “Fibre channel SAN Automation and orchestration” ,2018 Fibre Channel Industry Association.

[3] Priyanka Malviya, “A Study Paper on Storage Area Network Problem-Solving Issues”, 2016 International Journal of Computer Science Trends and Technology.

[4] M. Saravanamuthu and G. M. Kadhar Nawaz, "Maximum performance with minimum cost in data mining applications through the novel online data warehouse architecture by using storage area network with fibre channel fabric," 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, India, 2015, pp. 1-7, doi: 10.1109/ICCPCT.2015.7159498.

[5] L. Ochoa-Aday, C. Cervelló-Pastor and A. Fernández-Fernández, "Self-Healing Topology Discovery Protocol for Software-Defined Networks," in IEEE Communications Letters, vol. 22, no. 5, pp. 1070-1073, May 2018, doi: 10.1109/LCOMM.2018.2816921.

[6] Hewlett Packard Enterprise, “Data Center Automation and Orchestration with HPE Network Orchestrator”, Technical White Paper.

[7] K. Khalil, O. Eldash and M. Bayoumi, "Self-healing router architecture for reliable network-on-chips," 2017 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Batumi, Georgia, 2017, pp. 330-333, doi: 10.1109/ICECS.2017.8292030.

[8] Kadve, Anagha, “Trade Of Between SSD and HDD. International Journal for Research in Applied Science & Engineering Technology (IJRASET)”, 2016, 4. 473-475.

[9] MILANOVIC, STANISLAV & Mastorakis, Nikos. “Internetworking the Storage Area Networks”, 2002

[10] S. L. Aw, M. Saleh and W. A. H. A. Alsalihy, "Distributed iSCSI protocol over Hypervisor Storage on Local Area Network," 2009 IEEE 9th Malaysia International Conference on Communications (MICC), 2009, pp. 748-753, doi: 10.1109/MICC.2009.5431398.

[11] Z. Xin-ying, T. Xiao-dong and M. Lu-peng, "Zoning Implementations in Storage Area Networks," 2010 International Conference on Challenges in Environmental Science and Computer Engineering, 2010, pp. 155-157, doi: 10.1109/CESCE.2010.130.

[12] Y. Lee, R. Vilalta, R. Casellas, R. Martínez and R. Muñoz, "Auto-Scaling Mechanism in the ICT Converged Cross Stratum Orchestration Architecture for Zero-Touch Service and Network Management," 2018 20th

International Conference on Transparent Optical Networks (ICTON), 2018, pp. 1-4, doi: 10.1109/ICTON.2018.8473827.
[13] Y. Qiu, X. Qiu and Y. Cai, "Service function chaining policy compliance checking," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1-4, doi: 10.1109/NOMS.2018.8406194.
[14] U. K. Gaur, D. D. Sonvane, V. Kumar and R. Kalmady, "SANMAN-Management Software for Hyperscale SAN based storage system," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1-4, doi: 10.1109/ICCCNT49239.2020.9225598.

11.2Books

[5] Ulf Troppens Computer Science,Wolfgang Müller-Friedt,Rainer Wolafka,Rainer Erkens,Nils Haustein,Storage Networks Explained: Basics and Application of Fibre Channel SAN, NAS, iSCSI, InfiniBand and FCoE,2nd edition,Wiley, 2009