1) Explain the motivation behind the two forms of server placement (rack-mounted servers and blade servers). What is sacrificed to make a blade server more compact than a rack- mounted server?

Answer:

Servers came in form of either rack mounted servers or blade servers. These forms are optimized to reduce physical footprints and interconnection complexity. Such optimization is necessary in the face of a never increasing number of servers that need to be put in the constrained space of data center.

Blade servers are more compact than rack mounted servers. The smaller form factor is achieved by eliminating pieces that are not part of computing such as cooling. As a result, board is nothing but a computer circuit board with processor, memory, I/O and auxiliary interface. Blade is functional only if it is incorporated into rack which has missing modules. The chassis accommodates multiple blades. Chassis also provides a switch through which servers connect to outside. Point here is chassis can be fit into a rack like mounted server. (Blade vs. Rack vs. Tower Servers. (n.d.)).

2) Why is the use of the Ethernet technology particularly important to the data centers? [Hint: What need does the use of the Ethernet effectively eliminate?]

Answer:

Ethernet technology is particularly important to data center because of its potential to eliminate employing separate transport mechanisms (e.g., FC) for storage and inter processor traffic. (Data center bridging. (2019, April 9)).

3) Explain why NAS and SAN but not DAS are readily applicable to Cloud Computing. What are the limitations of DAS? Why is DAS suitable for keeping local data (such as boot image or swap space)?

Answer:

DAS has a limitation. Essential feature of a cloud is flexible allocation of virtual machines based on, among other factors, resource availability and geographical location. In case of DAS, when a virtual machine moves to new physical host, the associated storage needs to move to same host too, result in more band width and time. Since DAS is not subjected to network delay, it is suitable

to keep local data such as boot image and swap space. (Mackenzie-Low, B., Bruce, Hewlett-Packard, & Microsoft. (2014, May 22)).

4) Why is there a need for the Phy layer in the SAS architecture? How is it different from the physical layer?

Answer:

Physical layer deals with the physical and electrical characteristics of cables, connectors and transceivers. Phy layer deals with line coding, out of band signals and speed negotiation necessary for serial transmission. The name of the layer reflects the logical construct “phy” that represents transceiver on a device. (n.d.).

5) List the generic file-related system calls. Why in the NFS there is no RPC invocation for the close <file> system call? Under which circumstances other file operations may not result in an RPC invocation?

Answer:

Generic file related system calls are read, write and open.

First reason for not having RPC invocation for close system call is NFS protocol does not have the close routine because of original stateless design of servers to facilitate crash discovery. Second, in this case there is no file modification.

A remote file operation even if it has a RPC counterpart does not necessarily result in an RPC invocation. No such invocation is needed when the information is stored in the client cache which reduces the number of remote procedure calls and improves efficiency. Nevertheless, caching makes it difficult to maintain file consistency. (Network File System (NFS) Version 4 Minor Version 1 Protocol. (n.d.)).

6) What types of connection topologies are supported in FC-2M? Which of them is the most flexible? Why?

Answer:

The types of topologies that are supported in FC-2M are:

- Point to point
- Arbitrated loop

- Fabric/Switched/Switched Fabric

The flexible and powerful FC topology is the fabric or switched fabric. Additionally, to ports on each device, a fabric requires one or more hardware switches, making it more costly to implement than point-to-point or arbitrated loop. Involves a set of ports attached to a network of interconnecting to FC switches through separate physical links, switching network has a 24-bit address space structured hierarchically according to domains and areas. Each fabric connection has the full speed of a point-to-point connection. An attached port is assigned a unique address during fabric login procedure. the exact address typically depends on the physical port of attachment on the fabric. The fabric routes frames individually based on the destination port address in each frame header. A fabric works similarly to a phone system. (n.d).

7) How does the FCF respond to a discovery solicitation from the ENode?

Answer:

ENode selects a compatible FCF based on the advertisement and sends a discovery solicitation at which the capability negotiation starts. Upon receiving the solicitation, the FCF responds to the ENode with a solicited discovery advertisement, confirming the negotiated capabilities.

Once receiving the solicited discovery advertisement, the ENode can proceed with setting up a virtual link to the FCF. The procedure here is similar to the fabric login procedure in FC. Successful completion of the login procedure results in creation of a virtual port on the

ENode, a virtual port on the FCF, and a virtual link between them. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

8) Please answer the following four questions:

a) What features of TCP are leveraged in iSCSI?

b) Explain why these features are essential to SCSI operations.

c) Why is not SCTP used in iSCSI?

d) Why does iSCSI has to be deployed over an IPsec tunnel when its path traverses an untrusted network?

Answer:

a) iSCSI facilitates block-level initiator-target communication over TCP/IP networks. Features of TCP those are leveraged in iSCSI as multiple iSCSI nodes may be reachable at the same address,

and the same iSCSI node can be reached at multiple address. The output is that it is possible to use multiple TCP connections for a communication session between a pair of iSCSI nodes to achieve a higher throughput. (Cisco Press. (2010, July 28))
(Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

b) Internet Small computer System interface (iSCSI) protocol, the Internet Engineering Task Force (IETF) began working on iSCSI in 2000 and subsequently published the first iSCSI standard in 2004. Features are essential to SCSI operations because of dependable in order delivery, automatic re-transmission of unacknowledged packets, and congestion control. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

c) SCTP (Stream Control Transmission Protocol) which is a connection-oriented transport protocol and another IP protocol that provides reliable stream-oriented services similar to TCP. SCTP is especially designed to be used in situations where reliability and near-real-time considerations are important as well as it is designed to run over existing IP/Ethernet infrastructure. But at the time of standardization of iSCSI the SCTP was considered much new to be relied on.
(Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).
(n.d).

d) iSCSI by own self does not provide any mechanism to protect a connection or a session. All native iSCSI communication is in the clear subject to eavesdropping and active attacks. In an untrusted environment iSCSI should be used along with IPsec. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

9) What is connection allegiance? Explain how iSCSI sessions are managed.

Answer:

For the avoidance of this complication of the iSCSI admits a scheme knows as connection allegiance, accompanied this scheme the initiator can use any connection to issue a command even so must stick to the same connection for all ensuing communications. The iSCSI sessions need to be managed, and a large part of the session management is managed by the login procedure.

Successful completion of the login procedure results in a new session or addition of a connection to the session that already exists. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

10) Why the credential (as defined in ANSI INCITS 458-2011) itself cannot serve as a proof for access control? Give one example of a proof derived from the capability key?

Answer:

The credential is basically a cryptographically protected tamper proof capability, involving the keyed-Hash Message Authentication Code (HMAC) of a capability with shared key. To be more specific of the credential structure

<Capability Object Storage Identifier, Capability Key>

Where, Capability Key = HMAC (Secret Key, Capability|| Object Storage Identifier)

As an example: The standardized scheme derives a proof based on the capability key. the proof is a quantity computed with the capability key over selective request components according to the negotiated security method. Minimum it should be verifiable, tamper-proof, hard to forge, and safe against unauthorized use. A credential meets all but the last requirement i.e. no built-in mechanism to bind it to the acquiring client or to the communication channel between the devices to store and the client. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

11) Describe the three approaches to the block-level virtualization. Which approach is most suitable to the needs of Cloud Computing? What are the differences between the in-band and out-of-band mechanisms of the network-based approach along with their advantages and disadvantages?

Answer:

The three approaches to the block-level virtualization relying on where virtualization is done:

- **The Host:** Virtualization is dealt by a volume manager; the volume manager is responsible for mapping native blocks into logical volumes else while keep in track of the overall storage utilization which could be the part of operating system.
- **The Network:** Virtualization is handled by a special function in a storage network that may have a role in a switch. As this approach is transparent to hosts and storage systems as long as they

support the appropriate storage network protocols all depending on just well how the traffic control and application traffic are handled. It can be classified as in-band (symmetric) or out-of-band (asymmetric).

- **The Storage Device:** Virtualization is handled by the controller of a storage system as of the close proximity of the controller to physical storage as this approach reaches out to result in good performance. The drawback of being vendor dependent and difficult to work with many heterogeneous storage systems.

Network approach is most suitable to the needs of Cloud Computing.

In-band mechanisms of the network-based approach, virtualization function for mapping and I/O redirection is always in the path of both the control and application traffic.

-**Advantages:** The central point of control afforded by the in-band approach simplifies managing and support for advanced storage features such as snapshots, replication and migration. It can be applicable to capture the state of a virtual machine at a certain point in time, reflecting the run-time conditions of its components as example such as memory disks, and network interface cards in which the snapshot feature is of particular applicable to Cloud Computing.

-**Disadvantages:** The virtualization function could become a bottleneck and a single point of failure. A trade-off as in this case the performance of other virtual machines on the same host mat suffer when the snapshot of a virtual machine is being taken.

Out-of-band mechanism, virtualization function is in the path of the control traffic but not the application traffic.

-**Advantages:** This approach results in far better performance since the application traffic can go straight to the destination without incurring any processing delay in the virtualization function.

-**Disadvantages**: It does not lend itself to hold up advanced storage features. It imposes an extra requirement on the host to distinguish the control and application traffic and route the traffic approximately, which as a result the host needs to add a virtualization adaptor which incidentally also support caching of both metadata and application data to improve performance. Pre host caching faces the challenging problem of keeping the distributed cache consistent. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

12) Explain the difference (in terms of their capabilities) between the NOR flash- and NAND flash solid state drives?

Answer:

NOR flash is faster to read than NAND flash, but it's also more expensive and it takes longer to erase and write new data. NAND has a higher storage capacity than NOR. NOR storage density is limited. NAND devices are accessed serially, using the same eight pins to transmit control, address and data information. NAND can write to a single memory address, doing so at eight bits one byte at a time. NAND is more widely than NOR flash in digital cameras, portable music players, and smart phones. (Rouse, M. (2020, April 2).)

13) What are the three limitations that stand in the way of deploying the NAND flash solid state drives in the Cloud?

Answer:

The three limitations that stand in the way of deploying the NAND flash solid state drives in the Cloud:

- A write operation over the existing content requires that this content be erased first; which makes Write operations much slower than Read operations.
- Erase operations are done on a block basis while write operations on a page basis.
- Memory cells erase out after a limited number of write-erase cycles.

(Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

14) Explain the mechanism of consistent hashing used in Memcached servers.

Answer:

Consistent hashing is an idea that has been around for a while. It solves a common problem with sharded cache server clusters, which can be disrupted when a single node fails and sets off a festival of rehashing, key shuffling and cache-filling database calls. (Clark, B. (2014, February 18)). A result from a database query can be cached in a memcached server with the query string as the key. Even if each data item has a limited lifetime memcached does not implement garbage collection to actively reclaim memory. Be controlled on the size of DRAM available on a server caching the workload data may need more than one server, the hash table is distributed across multiple servers which form a cluster with collection DRAM. Memcached servers, by design, are neither aware of one another nor coordinated centrally. It is the job of a client to select what server

to use, and the client (armed with the knowledge of the servers in use) does so based on the key of the data item to be cached.

For selecting the same server for the same key, the hash table is distributed, a naïve scheme be as:

s= H(k) mod n,

where H(k) is a hashing function, k the key, n the number of servers, and s the server label,

which is assigned the remainder of the division of H(k) over n, the scheme works as long n is constant as it will more likely yield a different server when the number of servers increases or decreases dynamically as it would in Cloud Computing, which as a result cache misses abound application performance degrades and all servers in the latest cluster have to be updated.

This is undesirable, and so another scheme is in order. To this end, memcached implementations usually employ variants of consistent hashing to minimize the updates required as the server pool changes and maximize the chance of having the same server for a given key. The basic algorithm of consistent hashing can be outlined as follows:

- Map the range of a hash function to a circle, with the largest value wrapping around to the smallest value in a clockwise fashion;
- Assign a value (i.e., a point on the circle) to each server in the pool as its identifier49; and
- To cache a data item of key k, select the server whose identifier is equal to or larger than H(k).

The server selected for key k is called k's successor, which is responsible for the arc between k and the identifier of the previous server.

(Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

References

Blade vs. Rack vs. Tower Servers. (n.d.). Retrieved from https://www.serverwatch.com/server-trends/blade-vs-rack-vs-tower-servers.html

Data center bridging. (2019, April 9). Retrieved from https://en.wikipedia.org/wiki/Data_center_bridging

Mackenzie-Low, B., Bruce, Hewlett-Packard, & Microsoft. (2014, May 22). DAS NAS SAN Storage Technologies. Retrieved from https://www.petri.com/das-nas-san-storage-technologie

(n.d.). Retrieved from https://www.snia.org/sites/default/education/tutorials/2007/spring/networking/SAS-Overview.pdf

Network File System (NFS) Version 4 Minor Version 1 Protocol. (n.d.). Retrieved from https://tools.ietf.org/html/rfc5661

(n.d.). Retrieved from https://shodhganga.inflibnet.ac.in/bitstream/10603/196908/12/13_chapter%205.pdf

Faynberg, I., Lu, H.-L., & Skuler, D. (2016). Cloud computing business trends and technologies. Chichester, West Sussex: Wiley.

Cisco Press. (2010, July 28). Retrieved from https://www.ciscopress.com/articles/article.asp?p=484553

(n.d.). Retrieved from https://arxiv.org/pdf/1311.2630.pdf

Rouse, M. (2020, April 2). What is NOR Flash Memory? Retrieved from https://searchstorage.techtarget.com/definition/NOR-flash-memory

Clark, B. (2014, February 18). Consistent hashing with Memcached or Redis, and a patch to libketama. Retrieved from https://tech.wayfair.com/2014/02/consistent-hashing-with-memcached-or-redis-and-a-patch-to-libketama/