Object Storage

Diagram

Description automatically generated

Data Protection

* 1. i. No, there are no data read complexities. We only need to decide from which replica the data must be read from.

ii. Benefits—Users can route data reads across many machines to improve read performance.

Admins can save processing cycles when all reads are directed to a single replica.

Network load can be balanced as well as access speeds can be improved by placing the replica closer to the user’s location.

* 1. i. Identify the source and destination. Select table to be copied.

ii. Select replication method

iii. Update all other replicas and acknowledge once every replica is up to date.

iv. Final commit is done to the disk from the replicas.

v. Maintain quality control by monitoring the whole process.

* 1. i. Although the data is consistent but the whole process can be overall slow and costly in terms of utilization of resources.

ii. Also, more replicas will take up more storage space which will also make the cost to go up.

iii. The solution to these drawbacks is to not send acknowledgements and not to update all the replicas instant. The updated data can be written to the replicas eventually. This practice will not slow the process by simultaneously updating the replicas and not sending the acknowledgements to the clients immediately. Anyways, this method works at the cost of consistency during the initial phase of the operation.

I/O Virtualization

* 1. i. VirtIO – It is Frontend in Guest VM and backend in qemu.Data transfer take s place through Qemu and it emulates I/O accesses back and forth to guest, in a much simpler manner.

Graphical user interface, application

Description automatically generated

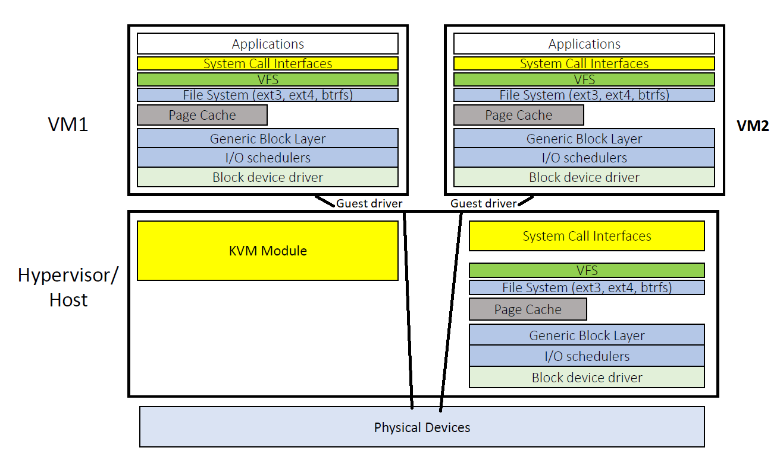
ii. vHost – normally Qemu user space process emulates I/O accesses from guest and vhost puts virtio emulation code into kernel in turn removing qemu from picture. Graphical user interface, application

Description automatically generated

iii. Hardware Support (Vt-d) – allows admin to assign I/o devices to VMs in any config. Graphical user interface, application

Description automatically generated

iv. Hardware Support (SR-IOV) – Allows single-root I/O virtualization. Each VM can dedicatedly access one virtual function.



* 1. i. Benefits- The main benefit would be that there would be 2 caches available where recent calls are temporarily being stored. This will be useful if similar system calls are made to the underlying VM then the cache will provide faster access times.

ii. Drawbacks- The draw back would be to maintain 2 different page tables inside both the active page caches. This will generate a lot of inconsistencies.

1. Network Virtualization
   1. i. A simple way to ensure isolation among VMs belonging to different tenants within a single host is to use VLANs.

ii. The main drawback of this isolation technique is that only packets with the same VNI (VXLAN network identifier) can talk to each other or else they would be isolated.

* 1. Yes, both VM1 and VM1’ can have the same IP address as they belong to different tenants which have distinct public IPs.
  2. i. First define gateways before starting the actual communication between the two VMs

ii. VM1 will be connected o net gateway1 and VM2 will be connected to net gateway2.

iii. Thus, now communication will take place like this-

VM1—netgateway1—netgateway2—VM2

And vice versa.

* 1. i. First we need to enable network virtualization for OVS, controller and net gateways.

ii. When network virtualization is enabled, we can turn on tunneling. Once tunneling is turned on, Tenant 1 & 2 would be able to talk to each other with the help of OVS & controller through net gateways or through tunneling.

1. Software Defined Networks
   1. i. When the 1st packet is received by the network, the OpenFlow switch will ask the controller for rules.

ii. The controller will find rules defined by Alice’s algorithm and will handle all the new arriving packets.

iii. The controller will insert all the rules defined in Alice’s algorithm into all the switches involved in the flow.

iv. Now, the controller will send a message to the OpenFlow switch indicating that all the rules have been installed and the packets can be forwarded by following the installed rules.

v. In this way, every packet will be forwarded by the Open Flow switch with the help of defined rules in Alice’s algorithm.

* 1. i. Short flows will suffer the most from the communication between SDN controller and Open Flow switches which is so expensive.

ii. In short flow, there are very few packets being transmitted. Now, when a single packet is about to be transmitted, a new rule/rules must be made along with other necessary things.

iii. This will increase the delay. Cost will also go up just for transmitting a single packet.

iv. Thus, to reduce the overhead, more packets must be sent at once where a little overhead won’t matter as the rules would be same for all the packets.

* 1. i. The controller can detect an unexpected rise in the number of requests coming from a single source. This can be a red flag which would indicate a Dos.

ii. Unregular spikes in traffic at unusual times coming from unknown device type, unidentified Ip address or location.

iii. Also, if there are multiple consecutive requests going to a single point might identify as a Dos attack.

All the above anomalies can be detected by the controller by always monitoring the traffic and recognizing out of order patterns. This is done without contacting the victim machine.

* 1. i. The controller will apply a threat rule to the suspicious source. When the threat rule is applied to the suspicious source. This will block the source if threat is detected.

ii. A source ip group can be made where multiple ips can added to which the threat rule would be applied.

* 1. SDN consists of many features which prove to be distinctive in detecting and mitigation DDoS attacks. These following techniques can be used to detect DDoS attack-
     1. Entropy
     2. Machine learning
     3. Traffic pattern learning
     4. Connection rate
     5. SNORT and OpenFlow integrated

Following techniques are used to mitigate DDoS attacks-

1. Drop Packets
2. Block Port
3. Redirection
4. Control bandwidth
5. N/w reconfiguration and topology change
6. Deep packet Inspection
7. Mac address change and/or IP address change
8. Quarantine or Traffic isolation

These above techniques can combined as per the implementation and used to detect and mitigate DDoS attacks.

1. Put it All
   1. Let’s say I’m building Amazon website which has multiple services.
   2. One of which is Amazon prime video.
   3. For website, Serverless computing option would be the best. It will dynamically handle client workloads and will auto scale as the user base grows.
   4. Amazon prime video is a streaming service which needs high availability of data and faster read times.
   5. This will require a huge database for storing the huge database of movies/ TV shows.
   6. To fulfill the above needs, I will use Nosql database. For eg. Dynamo DB.
   7. It will provide max scalability and performance.
   8. Like what amazon uses, amazon web service cloud would be best.
   9. This will maintain high availability and reduce access times for video playback and streaming high-definition content.
   10. Overall cost will also be reduced as the whole service is capable of auto scaling when needed. Also, necessary backups and auto selection of best server for any user trying to access content based on his location and other specifications.