2. Explain the advantage that paravirtualization provides for handling timers in virtual machines.

Answer:

In the paravirtualization the guest OS (Operating System) is modified so that it knows that it is running in a virtualized environment on top of a hypervisor as opposed to on top of native physical resources. The intention behind the modification of the operating system is to minimize the execution time required in performing the operations that are otherwise difficult to run in a virtual environment. There are various advantages of paravirtualization, the gripping and a notable advantage of paravirtualization is handling timers, most of the operating system trust clock interrupts for maintaining their internal timers and even an idle virtual machine needs to process the clock interrupts. Without paravirtualization the hypervisor would need to schedule timer interrupts for idle machines which would not be scalable. Whereas with the accompany of paravirtualization the VMC (Virtual Machine Code) changes the request a notification at the specified time. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)). (n.d.).

3. Explain how paravirtualization helps in minimizing access to APIC.

Answer:

Advanced Programmable Interrupt Controller (APIC) are used by x86-based multi-processor architecture for interrupt redirection in support of Symmetric Multi-processing (SMP). The access to APIC each time needs to be intercepted for virtualization which causes a lot of overhead and also expenses, and with paravirtualization it can achieve faster and efficient implementation as the many APIC access request can be replaced with just one hypercall. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

4. Find out if Linux (like Unix) has both the user-mode and system-mode stacks for each process it runs.

Answer:

There are 2 stacks because there are two CPU execution contexts. The user-mode stack will cater to your program with respect to creating stack frames for function, local variables, return addresses and others. When the CPU switches context to system mode, for instance during system call execution, it needs to access to kernel memory and data structures and so switches to using its system stack. And yes, Linux (like Unix) has both stacks user-mode and system-mode for each process it runs. (Faynberg, I., Lu, H.-L., & Skuler, D. (2016)).

5. Find out what "unscrambled" means in the description of the Intel LSL instruction (you can, for example, use the Intel manual referenced in the lecture).

Answer:

Through the Intel manual section 5.10.3 the LSL instruction, loads the unscrambled segment limit from the segment descriptor specified with the second operand (source operand) into the first operand (destination operand) and sets the ZF flag in the EFLAGS register. The source operand (which can be a register or a memory location) contains the segment selector for the segment descriptor being accessed. The destination operand is a general-purpose register. It is because that the limit field is spread across several bits within the GDT entry. So, basically "unscrambled" limit refers to the lower/upper limit fields put together into a single 20-bit limit. When the granularity bit is set, it also includes the 4K-multiplier

GDT structure of entry was extended from smaller previous versions, when protected mode was still only 16-bit, each entry consisted of a single 16-bit base and limit. Inclusion of the 32-bit mode, there needed to be a way to extend the base/limit without breaking backwards compatibility. Hence, Intel simply added new fields for the upper bits, which causes the base/limit fields to be discontinuous within the entry. (Intel® 64 and IA-32 Architectures Developer's Manual: Vol. 1. (n.d))

6. Read the following two papers:

- Carl Waldspurger and Rosenblum, M. (2012) I/O Virtualization. Communications of the ACM, vol. 55, No 1. January 2012. Pages 66-72; and
- Muli Ben-Yehuda; Xenidis, J.; Ostrowski, M.; Rister, K.; Bruemmer, A.; Van Doorn, L. (2007). The Price of Safety: Evaluating IOMMU Performance. Proceedings of the Linux Symposium on June 27th–30th, 2007. Ottawa, Ontario. Pages 225-230.

1) Explain the advantages and disadvantages of using I/O MMU by citing the appropriate text from the paper;

2) Research the Web to find what is meant by "carrier-grade hypervisors". What products are available?

1) Answer

I/O memory management unit (IOMMU) is translated to I/O virtual memory addresses in computer architecture, it is to correspond physical memory addresses making direct memory access by devices safe and efficient. Many benefits of virtualized systems depend on the decoupling of VMs logical I/O devices from its physical implementation, examples ranging from the ability to multiplex many VMs on the same hardware to advanced virtualization features as to live migration and enhanced security. The decoupling enables time and space multiplexing of I/O devices, applications of virtualization such as server consolidation or running heterogenous operating-system environments depend on this feature, also enabling VM feature known as live migration, such as the ability to suspend and resume a VM and to move running virtual machines between physical machines. The devices or machines which cannot support memory address long to address the entire physical memory can still address the entire memory through the IOMMU by avoiding the overheads associated with duplicating buffers to and from the peripheral's addressable memory area. One of the useful capabilities is device aggregation that is enabled by the IO virtualization where many physical devices can be combined into a single more capable logical device that is exported to the VM. It can be seen where multiple network interfaces can be combined to appear as a single faster network interface included in combining multiple disk storage devices exported as a single larger disk, and the network channel bonding. New features which can be added to existing systems by interposing and making transformation during virtual I/O requests, where

transparently enhancing unmodified software with new capabilities. Like a disk write can be transformed into replicated writes to multiple disks so that the system can tolerate disk-device failures. I/O channels can improve availability or balance load by changing mappings while copying storage contents across different I/O channels. Addition of new features to the existing systems by interposing and transforming virtual I/O requests transparently enhancing unmodified software with newly discovered capabilities such as a disk write can be transformed into replicated writes to multiple disks so as the system can tolerate disk-device failures. I/O virtualization many of them are designed to also improve system security, as firewalls and intrusion detection systems that employ deep packet inspection.

Downside of this optimization is that it protects other guests and the hypervisor from the guest but provides no protection inside the guest itself. Complex resource management issue as scheduling and prioritization are made known impacting performance across multiple VMs. There is also the challenge of defining appropriate semantics for virtual devices and interfaces especially incase of complex physical I/O devices. Some degradation of performance of translation and management overheads like in page table walks. (Gordon, A., Gordon, A., Technion, N. A., Amit, N., Har, N., Har, N., … IBM Research. (2012, March 1)). (Sugerman, J., & Ganesh Venkitachalam, B.-H. L. (2001, June 1)).

2) Answer:

Carrier Grade Hypervisor resolves issues related to virtualization with its management functions, real-time performance, high availability, fault tolerance and easy analysis. It is a set of specifications which detail standards of availability, scalability, manageability, and service response characteristics which must be met in order for Linux kernel-based operating system to be considered “carrier-grade” and known as Carrier Grade Linux. It integrates advanced technologies, such as intelligent priority control of CPU resources, disk I/O and network I/O, and memory access optimization to minimize virtualization overhead and hardware conflicts caused by accesses from multiple VMs. Featuring availability, upgrade capabilities, real-time behavior, minimum error recovery domains, systematic and uniform management services. Fail-safe logic a program improvement is applied to enhance fault tolerance capabilities, high availability and failover. Analysis features, such as VM resource usage tracing and comprehensive log collection, reduce

the time needed for failure analysis and virtualization software troubleshooting. The products available are:

- VirtualLogix Carrier Grade Hypervisors

- Oracle Solaris

- NEC's Carrier Grade Cloud Platform

- Bare-metal Xen Hypervisor

(n.d.).

(Waldspurger, C., & Rosenblum, M. (2012, January 1)).

7. Find out what hypervisors Amazon is using in EC2 and describe their major characteristics.

Answer:

Amazon EC2 uses Xen virtualization (bare- metal hypervisors in Xen). However, since 2017 it started to use KVM hypervisor called Nitro, but since Amazon has not fully given Xen up and still uses it. The major characteristics are:

- One of the features paravirtualization because paravirtualized guests are strongly relying on the Xen Hypervisor for support actions that usually require privileged access.

- Using a microkernel design, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.

- Taking advantage of embedded hardware features to lower datacenter electricity consumption by dynamically consolidating VMs on fewer systems and the powering off underutilized servers as demand for services fluctuates.

- It provides site recovery as it is easy to set up, recover and also has the ability to frequently test to ensure disaster recovery planning and services for virtual environments.

- It also supports live virtual machine migration and live storage migration. Live migration from one host to another allowing workload balancing avoiding of downtime and, move VMs and their associated virtual disk image within and across resource pools leveraging local and shared storage. (Badola, V. (2019, July 25)).

8. Examine the Amazon EC2 VM offer capabilities and particularly the Amazon Machine Image (AMI) ((https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html) and answer the following questions:

a. How (i.e., in what units) does EC2 measure the CPU power of a virtual machine and how is the unit in question translated into the power of the physical processors)?

b. What kinds of machine instances are there as characterized by the power of their respective CPUs, platform (i.e., 32-bit or 64-bit), memory, storage, etc.? Please list all the instances in the nomenclature along with their respective characteristics;

c. Which operating systems are available on the above systems?

d. What is an AMI and what is its relationship to an instance?

e. What are the components of an AMI?

a. Answer

ECU (EC2 Computing Units) is used for measuring the CPU power of a virtual machine. Many benchmarks and tests are used to determine the Computer Units translation into power of the physical processor and how it does that. As per the documentations, a single EC2 Computing Units is defined as the computer power of 1.0 to 1.2 GHz of a 2007 server CPU capacity. It equates to a certain amount of computing cycles in a way that is purportedly independent of the actual hardware. (Daly, D. J., & Daly, D. J. (1987)).

b. Answer

Amazon EC2 delivers a wide range of instance types that are probably optimized to fit various use cases. Most of the EC2 instance types have come up with various combinations like CPU, Storage, Memory and other networking capacities, providing, giving, flexibility in selecting the right mix of resources for respective applications. As for each and every instance Amazon EC2 provides a predictable and consistent amount of CPU capacity without the need for hardware making it easy to develop applications with an ease. There are various instances Amazon has come up with they are:

- **General Purpose Instances:**

- T2 instances is the best performed instances offering the baseline CPU performances providing with effective capability having the ability to burst all the performances directed by the CPU credits. The features of T2:

- Measures the bandwidth of the CPU by getting credits
- Built with the Extraordinary Regularity Intel Xeon Processors
- Helps the CPU perform at standard level
- Balances the compute, network possessions and memory
- It's a low cost AWS instance type used for ordering general types making you eligible to get an Free tier which is merely t2.Micro.

-**M5 Instances:** Instance types under the General Purpose EC2 Instance types is the M5 Instances which are the latest generation of the General-Purpose Instances. Its features are:

- Hosts 2.5GHz Xeon Platinum 8175 processor with latest Intel advanced Vector extension (AXV-512) instruction set.
- m5.24xlarge that offers of 96 vCPUs and 384GB memory.
- Higher EBS performance on small instance and optimized by default.
- Requires HVM AMIs to include drivers for ENA and NVMe.
- New light-weight Nitro systems that are a combination of hardware and lightweight hypervisors.

-M4 Instances: It is leading and best instances offering great network, memory balance by computing all the resources for several applications. The types are Large, Xlarge, 2xlarge,4xlarge, 10xlarge. Features includes:

-2.3 GHz Xeon E5-2868 v4(Broadwell) processors or 2.4 GHz Intel Xeon E5-2676 (Haswell) processors.

- EBS-optimized by default at no additional cost.
- Balance of computing, memory, and network resources.
- Support for Enhanced Networking.

- **M3 Instance:** M3 instance type is used to balance the network, memory and compute the resources according to it. Features of M3:

- A high-frequency Intel Xeon E5-2670 v2 (Ivy Bridge) processor

-SSD-based instance storage for faster I/O performance

-Balance of compute, memory, and network resources.

Compute Optimized Instances: These Compute-optimized instances are considered ideal for compute-bound applications. Batch processing workloads, Media transcoding, High-performance web servers, High-performance computing (HPC), Scientific modelling etc. are some of the applications that are the best-suited ones to run on these Instance types.

-C5 Instances: The instances are completely optimized for computing intensive workloads and delivers cost-effective high performance with low rates. Main use cases are high- performance web servers as mentioned above like bath processing, HPC, etc.

-C4 instances: Instances that are the addition to compute-optimized instances which are features with the max number of performance processors at the lowest amount of prices. They are suitable for the compute bound applications, depending on the custom processors that are optimized for EC2. The C4 instance types are dependent on the custom processors that are optimized for EC2. The Intel boost technology will help the clock speed of C4 instances to touch. EBS-optimized by default. It has the ability to control processor C-state and P-state configuration on the c4.8xlarge instance type. Only C4 and C5 instances require 64-bit HVM AMIs. They have high-memory (up to 144 GiB of RAM) and require a 64-bit OS. HVM AMIs provide superior performance in comparison to para-virtual (PV) AMIs on high-memory instance types.

- **C3 instance** type is greatly used to offer the CPU instance storage based on the SSD which has twice the memory and faster processors when compared to C1. These types of instances are well suitable for the applications that can derive the advantage from the compute capacity of memory, custom intensive application with high performing web servers.

Memory-optimized instances: They are designed to deliver the fastest performances for workloads that process large data sets in memory.

- **X1 Instances:** Defined as one of the latest additions of EC2 instance group that is intended to perform the high scale executing and in-memory applications over the AWS cloud. X1 instances will offer the lowest prices for each GiB of RAM and well suited to execute the in-memory databases and applications. Its features are:

    - It offers the lowest prices for each GiB of RAM and well suited to execute the in-memory databases and applications.

    - SAP certified instances to run the production environments perfectly.

- R4 Instances: It's a completely optimized high performance computing with memory intensive applications and mostly delivers the best price for GiB of RAM than R3. These are suited for many applications as; high performance relational, databases like MongoDB etc.

- **R3 Instances:** A fully equipped in order to run a memory-intensive application which is less expensive compared to other instances, offering greater performance with more bandwidth, supported latency, increased performance and great EBS optimization support.

Accelerated Computing Instances: The instances are known to be used where high processing capabilities as to providing access to hardware-based compute accelerators as GPUs (Graphical Processing Units) also known as the Optimized GPU instances.

- P3 Instances: P3 instances provide the required higher bandwidths, networking, powerful half, single, double-precision floating point capabilities and also 16GB memory per GPU. These instances use NVIDIA Tesla V100 GPUs and are specifically designed for general-purpose GPU computational needs using also CUDA or OpenCL programming models or machine learning framework.

- P2 Instances: The P2 Instances which use NVIDIA Tesla K80 GPUs and are designed specifically for the general GPU computing using the CUDA or OpenCL programming models. These Instances provide the highest possible bandwidth networking, powerful single and double-precision floating-point capabilities.

- support enhanced networking with Elastic Network Adapter
- EBS optimized by default
- support NVIDIA GPUDirect peer to peer transfers

- The p2.16xlarge Instance type provides the ability for an operating system to take control over the Control processor C-states and the P-states

- G3 Instances: The G3 Instances that come along with NVIDIA Tesla M60 GPUs that prove to cost-effective, highly performing platform for Graphics applications using DirectX or OpenGL. provide NVIDIA GRID Virtual Workstation related features as like support for 4 monitors with resolutions to the range of 4096 x 2160. It supports enhanced networking with the Elastic Network Adapter. The instances are EBS-optimized by default.

- F1 Instances: It offers hardware acceleration with field programmable arrays which are customizable making use of the FPGA developer AMI and AWS hardware development kit to create and invent the custom hardware acceleration techniques for using on the F1 instances. It includes the full-cycle FPGA development in the cloud.

Storage Optimized Instances: The storage instances are specifically designed to work with workloads that require the highest of the order of sequential read and write accesses to huge data sets on local storages. It

- H1 Instances: H1 instances are very well suited for applications as in data intensive workloads, or the system that require sequential access to large loads of data and also the applications that require high throughput access again to the humongous quantities of data.

- I2 Instances: Instances includes the High Storage instances providing very fast SSD backed instance storage optimized for very high random I/O performance and provide high IOPS at a minimum cost. It supports Enhanced Networking, High Random I/O Performance and High Sequential Read throughput.

- D2 Instances: D2 instances are specifically designed for workloads which are greater sequential write and get the read access for large data storage. These are well-suited for data warehouses, processing computing and Hadoop. These instances are optimized by EBS which offers dedicated block storage for your AWS account that ranges from 750 Mbps to 4000 Mbps with free usage also allowing users to access them regularly by achieving great network traffic.

(Technologies, M. (2018, June 18)).

c. Answer

The Amazon EC2 are:

-Amazon Linux,

-Ubuntu,
-Windows Server,
-Red Hat Enterprise Linux,
-SUSE Linux Enterprise Server,
-Fedora,
-Debian,
-CentOS,
-Gentoo Linux,
-Oracle Linux, and
-FreeBSD.
(Daly, D. J., & Daly, D. J. (1987)).

d. Answer

An instance is a virtual machine with particular specifications and OS that you choose while creating them. An AMI (Amazon Machine Image) is a complete backup of an instance. When you make AMI of an instance first, AMI Creation that has all of its launch configurations and secondly snapshot attached to this AMI which has disk backup of the instance. (Antoniou, L. (2015)).

e. Answer

AMI contains the template for the root volume for the instance. For example, an operating system, application server, and other required libraries. Majority component is a read-only filesystem image that includes an operating system like mentioned such as; Linux, Unix, or Windows, and any additional software required to deliver a service or a portion of it. (AWS Global Infrastructure. (2019)).

9. Find out about the pricing of the EC2 platforms and provide a few examples. (https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf)

Answer:

AWS provides different families of instance types based on different needs. It has four ways to pay for Amazon EC2 instances: On-Demand Instances, Reserved Instances, Spot Instances, and Dedicated Hosts.

AWS pricing is generally quoted for On-Demand Instances, paying for compute capacity per hour or per second, depending on which instances you run. There are not any no longer-term commitments or upfront payments are needed. It can be increased or decreased based on the compute capacity to meet the demands of application and can only paid for the specified hourly rates for the instance it is used. Users may also elect to use Spot Instances or Reserved Instances. Spot Instances allow users to take advantage of unused capacity within Amazon data centers. Spot Instances may be terminated at any time, following a 10s warning. The Spot price is set by Amazon EC2 and fluctuates periodically depending on the supply of, and demand for, Spot Instance capacity. Reserved Instances allow users to reserve capacity ahead of time at a discounted rate. The catch with Reserved Instances is that the user is contractually obligated to pay for the capacity whether or not it is used, and with terms ranging from one to three years, this can have disastrous financial implications if the needs of the organization change within that period. Dedicated Hosts can be bought for up to 75 percent off the On-Demand price helping to meet compliance requirements to reduce costs which can be done by allowing using existing server-bound software licenses. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server also helping with the compliance meet requirements. For example:

Standard 1 Year

T2. nano					
payment option	upfront	monthly	effective hourly	saving over on-demand	on-demand hourly
no upfront	$0	$3.29	$0.005	24%	$0.0059(per hour)
partial upfront	$18	$1.46	$0.004	32%	$0.0059(per hour)
all upfront	$34	$0	$0.004	34%	$0.0059(per hour)

C4. large					
payment option	upfront	monthly	effective hourly	saving over on-demand	on-demand hourly

no upfront	$0	$51.25	$0.0070	30%	$0.1(per hour)
partial upfront	$263	$21.90	$0.060	40%	$0.1(per hour)
all upfront	$515	$0	$0.059	41%	$0.1(per hour)

(n.d)

10. From the above exercise, you will learn that it is possible to create a free machine instance. Please, do the following:

1. Find out and document the essence of the respective Service Level Agreement (SLA); in particular write down what one needs to do in order to maintain this service free;
2. Describe the process (i.e., what exactly one needs to do) to create a free machine instance that could be used as a server. (Do not, however, create anything yet!)
3. Can you create a machine instance equivalent to your own PC and then transfer your own PC image there? If so, how would you achieve that?

1. Answer

A service-level agreement (SLA) defines the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-on service levels not be achieved. It is a contract between a cloud provider and the service user that outlines responsibilities, quality, and scope on both sides. To get the and maintain the service for free of Amazon EC2 need to sign up the free tier and get experience for 12-month period, create an account and use the provided service under certain usage limits. Steps included are:

-Sign up for AWS account

- To provide credit card information and billing address, until the free usage exceeds the limits and until not to be charged for the services.
- Finally, get started with AWS Cloud services and choose any of the products listed under the free tier service.

(Overby, S. (2017, July 5)).

2. Answer

To create a free machine instance that could be used as a server one can follow these steps:

- Create an instance of Amazon EC2 which can be used as a server for hosting an application on the cloud.
- Create a server for the database which will be a database instance.
- Following the above steps, a web application can be deployed on the server.
- Then load balancing and scaling needs to be done so that the traffic is distributed across the number of servers or applications servers.
- At last, the user can associate or use a name with your web application. (n.d).

3. Answer

It is possible to create a machine instance equivalent to your own PC and transfer your own PC image there. This can be achieved by creating an EC2 instance on the Amazon Cloud and host it as a server. Then, need to connect the PC to that server and then transfer the image. (n.d.)

Reference

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

(n.d.). Retrieved from https://www.virtualbox.org/manual/ch10.html
Intel® 64 and IA-32 Architectures Developer's Manual: Vol. 1. (n.d.). Retrieved from https://www.intel.com/content/www/us/en/architecture-and-technology/64-ia-32-architectures-software-developer-vol-1-manual.html

Gordon, A., Gordon, A., Technion, N. A., Amit, N., Har, N., Har, N., … IBM Research. (2012, March 1). ELI: bare-metal performance for I/O virtualization. Retrieved from https://dl.acm.org/doi/10.1145/2248487.2151020

Sugerman, J., & Ganesh Venkitachalam, B.-H. L. (2001, June 1). Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor. Retrieved from https://dl.acm.org/citation.cfm?id=715774

(n.d.). Retrieved from https://www.vmware.com/files/pdf/techpaper/vmware-vcloud-nfv-high-availability.pdf

Waldspurger, C., & Rosenblum, M. (2012, January 1). I/O Virtualization. Retrieved from https://cacm.acm.org/magazines/2012/1/144808-i-o-virtualization/fulltext
Badola, V. (2019, July 25). AWS AMI Virtualization Types: HVM vs PV (Paravirtual VS Hardware VM). Retrieved from https://cloudacademy.com/blog/aws-ami-hvm-vs-pv-paravirtual-amazon/

Daly, D. J., & Daly, D. J. (1987). Economics 2: EC2. Retrieved from https://aws.amazon.com/ec2/faqs/#What_is_an_EC2_Compute_Unit_and_why_did_you_introduce_it, https://www.datadoghq.com/blog/are-all-aws-ecu-created-equal/) b. Amazon EC2 gives the option of choosing between different

Technologies, M. (2018, June 18). EC2 Instance Types: A Complete AWS EC2 Instance Info 2020. Retrieved from https://mindmajix.com/aws-ec2-instance-types

Daly, D. J., & Daly, D. J. (1987). Economics 2: EC2. Retrieved from https://aws.amazon.com/ec2/faqs/

Antoniou, L. (2015). Marketplace. Retrieved from https://aws.amazon.com/marketplace/b/2649367011?ref_=header_nav_category_2649367011

AWS Global Infrastructure. (2019). Retrieved from Machine Learning in the AWS Cloud, 151–160. doi: 10.1002/9781119556749.ch7

(n.d). Retrieved from https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf

Overby, S. (2017, July 5). What is an SLA? Best practices for service-level agreements. Retrieved from https://www.cio.com/article/2438284/outsourcing-sla-definitions-and-solutions.html

(n.d.) Retrieved from https://aws.amazon.com/ https://aws.amazon.com/premiumsupport/knowledge-center/import-server-ec2-instance/