Virtualization Technique for Effective Resource Utilization and Dedicated Resource Management

Megha V R[1], Dr G N Srinivasan[2]

[1]*Software Engineering, R.V College of Engineering, Bengaluru, Karnataka, India*

[2]*Professor –RV College of Engineering, Bengaluru, Karnataka, India*

Abstract- ***In these modern days, for numerously triggering trendy application with various technology adoption leading to growth in the need of the enormous resources such as CPU's, Memory, NIC ports, HBA ports and so forth. For this growing need for resources, which in turn impacts both the users and also many organization in a cost effective way, Also resources may not be utilized completely always leading to wastage.***

Virtualization with commodity hypervisors holds the promise of solving this problem of logical partitioning of resources in a single box. What commodity hypervisors cannot do is create efficient partitions of dedicated resources which are not shared with other partitions. This capability is critical in certain enterprise class environments.

1. Introduction

Secured partition is a software layer consisting of a Partition Machine Monitor (PMM), its associated service partitions, and firmware/drivers provided for the guest partitions. Secured Partition creates and manages guest partitions which have dedicated non-shared computing resources[1]. These s-PAR guest partitions will be referred to as Soft Machines (SMs).

This is implemented as a hardware assisted virtual machine which is optimized for non-shared computing resources. Each SM provides the capabilities of a physical server and is isolated from other partitions through the containment properties of the underlying Ultravisor software layer.

Secured partition can operate on top of BIOS along with the usage of Ultravisor to perform tasks such as virtual address to physical address translation, physical device emulation, and physical-to-virtual interrupt translation.

An improved feature for Secured partition includes the virtualization of the processor's native virtualization instructions itself. [1]Thus Secured partition is capable of hosting commodity hypervisors, such as VMware©, Xen©, and HyperV, which require these instructions for operation. With this additional feature, the Secured partition operating environment will be able to directly host Windows, Linux, and any other operating systems in logical partitions alongside partitions with commodity hypervisors hosting their own operating systems.

2. Background Research

Hypervisors are becoming popular because of their ability to make more efficient use of server resources through virtualization and sharing of resources among the logical partitions (virtual machines) that they create. S-Par technology has the ability to be extended to this class of logical partitioning but initial design focus is on the creation of secure logical partitions with dedicated hardware resources (*i.e.*, CPUs, memory, and I/O). This capability is critical in many enterprise class environments.

3. Methodology

Each operating environment or partition is visible to the data center as an independent server capable of hosting any operating system which is supported by the underlying hardware. Not only the operating system also other hardware's such as NIC HBA Cores Chassis can also be virtualized. Secured partition is unique in two respects: (1) it has an advanced architectural design which makes it more scalable and secure than current logical partitioning technologies and (2) it is the only logical partitioning software in its class that is based on Intel's x64 processors. Other logical partitioning technologies in this class are developed by IBM (LPARs) and SUN (LDOMs) and execute only on each company's respective proprietary processor technology.

4. Architecture

Figure 4.1 displays the environment of a logically partitioned server. The hardware resources, which lie at the bottom of the stack, consist of all of the hardware resources of a single server. This includes all components for processing (processors, cores, chip sets), memory, and IO (storage and networking).

The Ultravisor kernel executes at the bottom of the software stack and maintains complete control of memory management (for both internal server memory and IO memory mapping), actual IO port space, configuration space, and interrupts for all components which reside higher in the stack. Above the Ultravisor kernel reside machine monitors (UMM, PMM, and VMM

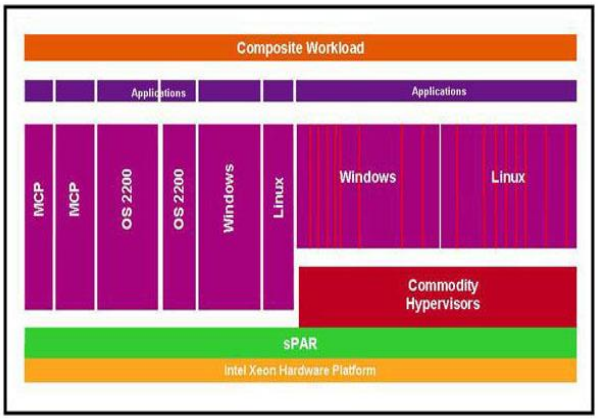

Figure 4.1: Virtualization system model

Which create all logical partitions in the server. The components of the stack encased by the lavender area in the figure comprise the two tiered stack of s-Par.

Secured partition has its own machine monitor (PMM) that manages the s-Par sVMs and guest SMs. The sVMs provide system management, command, console, and IO services for the SMs. The PMM is optimized to manage dedicated computing and IO resources.

Secured partition creates and manages guest SMs which have dedicated, non-shared resources. The SMs have properties and features which support ClearPath operating systems and enable mainframe enterprise class IO control and recovery. The virtual machine monitor in the figure, VMM, creates and manages virtualized logical partitions. [2] The VMM is optimized to manage shared computing and IO resources. Multiple PMMs and/or VMMs can run concurrently. A separate machine monitor instance is activated for each guest of each PMM and/or VMM. Each machine monitor instance is only aware of the resources assigned to it and the Ultravisor maintains isolation of all of the partitions.

5. Advantages

5.1 Security: Boundaries enforced by hardware rather than by software

5.2 Error containment: Hardware mechanisms prevent propagation of fatal errors across boundaries

5.3 Performance: Better and more predictable. Direct access to cores, memory, and I/O slots

6 Description Modules

6.1 Hardware Elements

Secured partition based partitioning can run independently in one or more hardware partitions. Secured partition is not dependent on hardware partitions and is capable of running on any server with the required processor hardware assisted virtualization technology.

6.2 Guests

A guest utilizes a portion of host resources generally to perform useful (to the guest) work. From the s-Par perspective, guests are pure consumers and provide no useful work to other partitions.

6.3 Virtualization

[3] The key premise of server virtualization is to provide virtual instances of basic computing resources. It is not so much a new layer of new abstractions, as it is an extension of an existing platform firmware layer.

6.4 Service Partitions

Service partitions may be software partitions or virtual partitions. Service partitions are partitions of the host that provide services for guests and other services as required. Service partitions are provided by multiple implementations and different layers of the architecture. Multiple service partitions can be configured to provide redundant services to prevent single points of failure.

7. CONCLUSION

The Secured partition solution is not constrained to a proprietary hardware platform, and its partitions are capable of supporting any operating system which can be hosted by Intel Xeon x64 processors. In addition, Secured partition is capable of supporting a virtualization environment similar to Micro partitioning which can create VMs which share resources alongside logical partitions with dedicated resources.

REFERENCES

[1]CombiningVirtualization,Resource Characterization, and Resource Management to Enable Efficient High Performance Compute Platforms Through Intelligent Dynamic Resource Allocation D. Roe_, D. Thompson_, and M. Wong_ Sandia National Laboratories MS _9159 / _9152 P.O. Box 969, Livermore, CA U.S.A.

[2] Chris Wolf, Erick M. Halter, *Virtualization: From the Desktop to the Enterprise*, Apress 2005.

[3]Combining Virtualization**,** resource characterization**, and** Resource management to **enable efficient high performance platforms through intelligent dynamic** resource **allocation**. P. Pébay; D. Roe; D. Thompson; M. Wong 2010 IEEE International Symposium on Parallel & Distributed Processing, Workshops and Phd Forum (IPDPSW)