Glossary of Virtualization Technologies

Address-Space Compression: The challenges of protecting portions of the virtual-address space and supporting guest access to them.

Address Translation Services specification (ATS): Specifies standard means to allow caching of device specific direct memory access transactions in the endpoint device.

Binary Translation: An approach to create the perception that the hosted operating system is communicating directly with the hardware. The virtual machine monitor makes changes to the binaries of the operating system as they are loaded into the virtual machine. The approach is common in commercial products but has the singular limitation that only specific versions of the operating system can be loaded.

Direct Memory Access (DMA): Allows a device with appropriate hardware to directly access system memory for data transfer without the intervention of the CPU.

Endpoint Access Control (EAC): Protects access to enterprise services contingent on the client platform being in an acceptable state. Also known as the Network Access Control.

Great Physical Address (GPA): The guest operating system's physical address range.

Host Physical Address (HPA): The host system's real physical memory addresses according to the device's assigned domain.

Lightweight Virtual Machine Monitor (LVMM): A virtual machine monitor using Intel® Virtualization Technology to partition a client platform into two execution environments. One is the user's virtual machine that can run an operating system and applications that the user needs and the second is a service partition that runs a service operating system in an isolated environment.

Native: Performance results from running a workload on a non-virtualized system.

Para virtualization: An approach to create the perception that the hosted operating system is communicating directly with the hardware. The technique, which does not work with off-the-shelf operating systems, requires changes to the source code of the operating system, especial the kernel so that it can be run on the specific virtual machine monitor.

Physical address extensions (PAE): A processor feature that allows for up to 64 GB of memory to be used in 32-bit systems, given the appropriate OS support.

Policy Decision Point (PDP): Interprets the access policy, parameters of acceptability, developed by the enterprise and controls the Policy Enforcement Points.

Policy Enforcement Points (PEPs): Collects and processes intrusions, security alerts,

violations, and other abnormal behaviors from a variety of systems and responds by controlling access.

Protection Domain: An isolated environment containing a subset of the host physical memory.

Ring Deprivileging: A technique that runs all guest software at a certain security level greater than 0 and defines what actions can be performed by specific processes.

Virtualization: The ability to run multiple applications and operating systems on a single server or PC.

Virtual Machine (VM): An abstraction of the computer hardware that allows a single machine to act as if it were many machines.

Virtual-machine control structure (VMCS): A new data structure that manages virtual machine entries and exits and processor behavior in VMX non-root operations.

Virtual Machine Monitor (VMM): The control system at the core of virtualization. It acts as a host, presents guest software with an abstraction of the physical machine and retains selective control of processor resources, physical memory, interrupt management and data input-output while maintaining full control of the platform hardware. Also known as a hypervisor.

VMX: Performance results from running a workload on a fully virtualized guest that uses Intel® Virtualization Technology.

VMX/Native: Performance percentage, showing the delta between fully virtualized and native performance.