Enterprise Architecture: Virtualization

Kirk Hausman
Assistant Commandant, Texas A&M University, College Station, Texas, U.S.A.

Abstract
This entry examines many different types of virtualization. Identification of scenarios that may benefit from cloud computing are provided. Best practices in virtualization are reviewed.

The Greek philosopher Plato formulated the *theory of forms*, which is based on the concept that the world of experience and sensation is merely a reflection or representation of a more fundamental abstract form of reality. The modern enterprise network embodies a form of Plato’s theory, creating electronic copies of physical documents that can be duplicated and re-created at will or constructing entire virtual worlds with their own physics models and constraints. Even technology is becoming more a reflection of purpose and function, compared to physical systems dedicated to a single task or purpose.

This entry will examine the virtualization of services and technologies within the extended network enterprise. While I will not attempt to rival Plato’s work with a “theory of virtualization,” it is worth noting the continued shift from physical representations of technology toward more fundamental abstracted forms that consume less power and provide greater flexibility than their physically bound predecessors.

VIRTUALIZED SERVICES

Virtualization of services and functions is not a wholly new concept. Answering machines, for example, provided a virtual replacement for human answering services, and have since been replaced in turn by voice mail systems. Modern enterprise collaboration systems such as the Microsoft Exchange platform with its Live Communication Server option can even take a voice message, perform automated voice recognition, and transmit the resulting text and audio to an individual’s mailbox for easy review on the recipient’s device of choice.

Other services, such as virtual faxes, print spoolers, and virtualized data storage reduce the technology equipment footprint within the enterprise while extending access to consumers throughout the enterprise. A single automated fax service can serve the entire enterprise, providing electronic facsimiles of documents without requiring consumables such as paper and ink cartridges and without delays involved with distribution of physical document copies.

Automated monitoring and update services allow management of maintenance and security functions without requiring direct access to individual physical systems. Such virtualized services provide a mechanism for direct support of thousands of distributed systems by a handful of support technicians, gaining efficiencies in personnel costs and user downtime. Additional support functions rely on virtualization for management over very large numbers of systems that may be distributed across many sites in a global network.

VIRTUALIZED APPLICATIONS

Virtualization of applications involves the creation of an application package that is made available to users automatically or on demand. Applications can be automatically deployed to a user’s system based on role membership, ensuring that the user’s desktop experience remains the same regardless of which system is used to access the enterprise network. Coupled with virtualization of user file storage using a distributed file share and/or user folder redirection, users need never worry about data and application availability. These services also allow rapid deployment of replacement or upgraded equipment, because the user experience is automatically applied to any system when the user first logs onto a new system.

Virtualized applications allow multiple versions of an application to be available simultaneously on the same system, ensuring continuity of operation for legacy applications depending on second-party add-ons or applications. For example, an older form of a Java virtual machine (JVM) might be required for Application X to operate. Users could then automatically use the older browser and the JVM when accessing Application Y.
X, but use newer versions of each during normal operations. Updates become easier in a virtualized application environment, by allowing an updated package to be uploaded onto the application virtualization server, which is then automatically downloaded to a user’s system upon next use of the appropriate program or file type.

An additional efficiency provided by virtualized application environments is the potential to reduce software licensing costs by providing a reduced pool of concurrent licenses, which are claimed upon application access and freed up for reuse when the application is closed. Rather than installing an expensive application on each computer system across the network, or limiting application availability to a select group of workstations, users can be added to application virtualization groups to gain automatic package availability using a smaller pool of concurrent licenses.

VIRTUALIZED DESKTOPS

The next level of virtualization involves the user experience to include the entire desktop, encompassing the operating system and all other functions into a virtualized setting mirroring the experience of sitting at a dedicated workstation desktop environment. This is somewhat similar to older mainframe operations, when terminals provided keyboard input and returned displayed output from processes that ran entirely within the mainframe’s central processing unit (CPU), memory, and storage resources.

Remote Desktop Clients

Client systems accessing virtualized desktop environments may use “dumb” terminals similar to older mainframe configurations or “thin” clients with only sufficient resources for input, output, and network communications. “Thick” clients may have local storage and applications to shift processing power from the server, while mobile computers with their own applications and configuration details may be used to access organizational services and data while limiting exposure.

Updates to a virtualized desktop environment occur at the host system, allowing rapid update to applications and system settings from a centralized data center. Remote desktop connections can be made to in-place dedicated systems for availability in mobile or remote settings, or may connect to one of many virtualized desktop sessions maintained on a powerful virtualization host residing in the data center. Virtual desktop infrastructure implementations include additional services to facilitate user reconnection to virtual desktop sessions left in operation.

A virtualized desktop environment can allow continued use of legacy desktop hardware that is no longer able to run most applications, by allowing the older hardware to function as a thin or thick client for a remote virtual desktop running on hardware with sufficient resources to support more recent applications and services. Extending the life cycle of individual systems this way reduces procurement costs and the environmental impact of computer manufacturing and disposal processes.

Virtual Appliances

Virtual appliances consist of preconfigured virtual systems with their own operating system, applications, and settings. These systems can provide an excellent mechanism for distributing entire software environments without requiring installation of packages on a host system, beyond the virtualization service itself (called a hypervisor). Demonstrations of new applications within a preconfigured virtual appliance require only a copy of the virtual hard drive files and minor network configuration to be up and running on a client’s test bed.

Virtual appliances and PC-hosted virtual machines can also allow a single workstation to provide access to multiple computing platforms simultaneously. The popular Apple Macintosh system includes the Parallels virtualization environment, allowing native Windows functionality within a virtual PC hypervisor. Newer forms of Microsoft’s Windows platform include the Windows on Windows virtual hypervisor for backwards compatibility in legacy applications. Use of a PC hypervisor such as the popular VMWare service can allow a single workstation to support as many different virtualized desktop configurations as system resources allow, together with options for capturing point-in-time snapshots for automatic rollback during testing and development. This can greatly reduce design time by eliminating the need to completely reload a test system each time a setting or application function is altered and by providing developers with multiple versions of operating systems, browsers, and application software suites with which to test the new application under development, without the need for individual physical hardware systems for each.

VIRTUALIZED SERVERS

Virtualization of multiple physical servers onto more powerful centralized hosts within the data center can provide significant cost savings in terms of hardware, energy, and cooling requirements. Since many servers can operate at a reduced level during off-peak hours, consolidation onto a smaller number of hosting
machines can reduce the power consumed by idling systems. Each virtualized server is merely a collection of files, rather than a dedicated hardware platform with storage, CPU, and memory of its own, allowing more efficient utilization of available resources as well as portability across hardware hosts, as shown in Fig. 1.

Automatic load balancing across hosting farms can ensure that spikes in demand are met with adequate resource allocation to individual virtualized servers. Resource management requires strict policies and attention to operational thresholds in order to protect against “virtual sprawl” in the data center and alignment of dedicated resources within each host to the needs of its virtual machines. Because virtualization allows separation of hardware and software refresh cycles, policies must also be put in place to handle software update and retirement of virtual as well as physical systems in order to properly secure the network and to limit complexity in support requirements.

VIRTUALIZED NETWORKS

Virtualization of networks beyond simple desktops and servers can afford an enterprise opportunities for modeling, testing, and defense. Construction of a test network matching the full suite of applications and services within a large enterprise can be a very costly matter, while a complete virtualized network with identical configurations and settings might be managed using only a single powerful host. Each virtual system in the test network might have reduced processing power compared to its production equivalent, but can be easily rolled back to a previous snapshot in the event of corruption or failure during test. Virtualized networks can also be used for penetration testing without concern for disruption of the production network, while “decoy” networks with automatically generated traffic and network utilization can allow would-be network attackers an environment in which their efforts are encapsulated and recorded for later review of attacking methods. These decoy networks, called honeynets, appear to be valid, active network environments but are actually virtual sandboxes, separate from the production network environment with only simulated use and data files present for access by an attacker.

CLOUD COMPUTING

When the network, servers, and infrastructure are virtualized and resources are made available automatically from a pool of systems, the result is termed cloud computing. Cloud computing is a natural extension of distributed grid processing when combined with the virtualization of services and operating systems. A cloud computing client might be allocated up to eight processors, 20 GB of RAM, 300 GB of storage, and up to four websites supported by four databases. Without needing to know the details of the location and type of these resources, an authorized user might request a new Web reporting application supported by 40 GB of storage, 4 GB of RAM, and two CPUs. Because these resource limits fall within the user’s allocated constraints, the resources can be automatically provisioned without interaction with tech support.
Comparing Cloud and Traditional Application Life Cycles

Fig. 2 illustrates a traditionally developed application, passing through the design phase, increased capacity requirements during testing, reduced requirements during rollout, and the highest resource need during its active life cycle. Pain points occur when escalating resource need exceeds available resources, requiring hardware upgrades or application migration to provide needed application host resources (represented by the dark gray boxes). Following end of life, applications retained for reference purposes continue to consume the same resources unless migrated again to other equipment.

Fig. 3 illustrates application development in a virtualized or cloud computing environment. Cloud computing resources can flex as needed, allowing the easy scaling of prototype solutions through testing and up to production levels with nothing more than an automated request for additional resource allocation. If expected capacity far exceeds actual capacity requirements, resources can be scaled back and allocated to other purposes through the same mechanism.

Types of Clouds

Because the term cloud computing refers to the configuration of resource availability more than a specific configuration of hardware and software, there are several common types of cloud computing that may be employed by an organization.

- **Public clouds**—These clouds are hosted on publicly accessible systems, available for Internet access from anywhere in the world. Examples of this type of cloud include Google’s Gmail and Microsoft Live Hotmail services. Most public clouds share host servers across multiple client cloud resource pools.
- **Dedicated clouds**—Like public clouds, dedicated clouds are hosted on systems available via Internet connectivity. Dedicated clouds isolate instances by restricting resource use by a particular client to a specific subset of hosting systems. Because the resources are dedicated to a particular client, these services are generally more costly than public cloud implementations.
- **Private clouds**—A private cloud is one that is typically maintained within an organization’s own network, or isolated in some manner from external access. Cloud hosting services may place dedicated hardware within the organization’s data center, or an organization might construct a private cloud using its own hardware.
- **Hybrid clouds**—Hybrid clouds may provide a mixture of dedicated, public, and private cloud resources. Management of disaster recovery (DR) functions, service-level agreements for resource and network availability, and other characteristics must be carefully negotiated in order to obtain the greatest value from a hybrid cloud configuration.

CLOUD FLEXIBILITY

The flexibility of resource assignment within a cloud computing environment can be very attractive to operations that require a variable amount of resources. Examples of scenarios where this availability provides greatest benefit include:

- **The bump**—This scenario, illustrated in Fig. 4, includes a sudden unexpected spike in activity. Examples include sudden surges in activity during emergencies or following the mention of a site on a popular news aggregator, causing a flood of interest outside normal access levels.
- **Cyclic surges**—This includes resources that are only necessary on a cyclical basis but are unused during other times, as shown in Fig. 5. Examples include mandatory training just before evaluation periods and end-of-month or end-of-year reporting cycles.
- **Rapid growth**—This scenario includes any application access that expands rapidly beyond expected resource requirements, as illustrated in Fig. 6. Prototypes placed into limited use may see rapid adoption enterprise-wide, or Internet information sites may experience sudden expansion of interest following initial exposure.
BEST PRACTICES

Due to the relative newness of cloud computing, best practices continue to emerge and evolve. A few of the more common practices include:

- **Setting standards**—Cloud resource hosting services, such as the Amazon EC2 or Microsoft Azure standards, do not work well between technologies. Selection of a cloud computing standard will ensure that developed applications and services interoperate well with other cloud resources and with in-place technologies in the enterprise.

- **Controlling costs**—Because cloud service vendors scale costs based on resource allocation and segmentation, enterprise cloud service hosting should be negotiated using the most economical model for existing and near-term requirements. Cost models include levels of dedicated resource and bandwidth availability, longer-term contracts providing a set level of resources for a fixed cost, or resource pools that may be used across a variable period of time and renewed when consumed. More complex hosting costs include per-transaction micro fees, upload/download transaction costs, incremental storage costs, and specialized costs for restrictions of data and DR backups to specific geopolitical boundaries.

- **Privacy requirements**—Contracting cloud services should include statements of where data will be stored, where DR copies may be made, and

---

**Fig. 4** A comparison of capacity requirements due to a short-term unexpected bump in activity.

**Fig. 5** A comparison of capacity requirements created by cyclical surges in activity and access. Note that in virtualized cloud scenarios, capacity can be preprovisioned to meet expected need during successive cycles.
conditions for reporting when data is exposed or transferred to new hosting facilities. Because larger hosting firms may make use of environmental cooling by moving data center operations north during summer months, requirements for legal data discovery and open records requests may fall under different legal systems. Contracts should include details regarding reporting discovery actions and other forms of external data access.

- **Compatibility**—To best use available application development skills and tools, cloud computing platform standards should be selected to integrate well with existing enterprise technologies. Mid-migration between local and cloud-hosted e-mail services, for example, is much less problematic if both services are compatible and can interoperate transparently. Because cloud services trade off flexibility and customizability for protection against potential conflict with shared resource clients, some applications may prove to be unable to migrate into the cloud and so a standard for interoperability between cloud and local applications is mandatory.

**SUMMARY**

This entry has addressed the virtualization of services, applications, workstations, servers, networks, and migration of entire infrastructures into the cloud. Virtualization practices provide significant cost savings by reducing hardware, energy, and cooling costs. Virtualization provides reductions in support requirements, as well as ease of recovery following system loss or upgrade.

The steady migration of resources into the cloud reduces tech support requirements for new initiatives, and eases resource extension to meet growing or widely varying requirements. Care must be taken to ensure that virtualized resources are managed, updated, and retired just like their physical system counterparts.