

Office of Technology Strategies (TS) Architecture, Strategy & Design (ASD)



A VA Executive's Guide to Virtualization

INTRODUCTION

Perhaps the most recognizable application of virtualization technology is cloud computing. Many senior executives are familiar with the excitement that has been built up around "the cloud" in recent years. However, they may find sales pitches lack the level of detail needed to assess whether cloud computing fits their organization's needs or strategic vision. Even if full-scale cloud computing is not a fit for your line of business, there are many different ways to use the virtualization technology behind cloud computing to positively impact service delivery and resource allocation.

VA is increasing its investment in virtualization and virtualized environments for use across the administrations and central business offices. Understanding key aspects of virtualization and virtualized environments, including technical terminology, is critical to having the ability to make decisions that will better position

VA to meet its strategic goals. This CTS Note highlights key topics and terms that help provide that understanding when faced with technically complex discussions about virtualization and virtualized environments.

WHAT IS A VIRTUALIZED ENVIRONMENT?

Traditionally, computing environments are made up of any number of servers that each run only one operating system (OS) and application at a time. Because of this narrow usage, the servers tend to utilize only a very small amount of their computing capacity. If there is a business need for several applications or several OSs, the IT infrastructure required in this traditional architecture can be quite wasteful by using an inordinate amount of energy, physical space, and monetary resources for support.

In a virtualized environment, the OS and application bundle, known as a "virtual machine," run on top of the existing

This newly established office within OIT's Architecture, Strategy & Design (ASD) interacts not only with the ASD pillar offices, but also with multiple stakeholders within OIT and with strategic offices across the enterprise. TS works closely with IT and business owners to capture business rules and provide technical guidance as it relates to Data Sharing across the enterprise, specifically for inter-agency operability.

hardware. However, virtualization software allows several virtual machines to run independently of each other on the same hardware (see Figure).

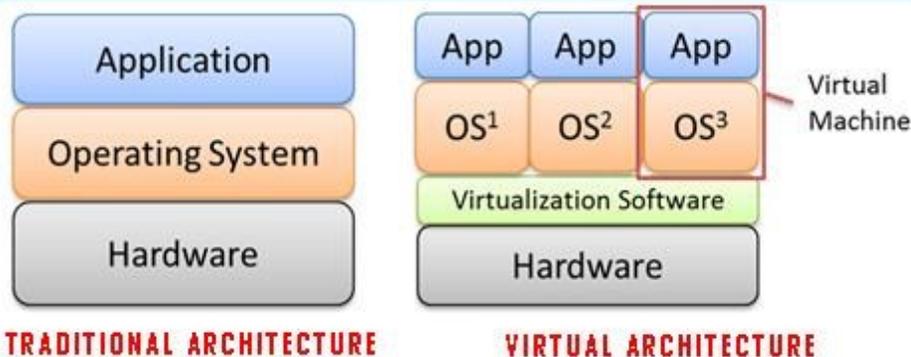
WHAT ARE THE SERVICE OFFERINGS?

There are several different business models in which the technical concepts of virtualization are employed:

Server virtualization – The base hardware is virtualized, allowing multiple guest operating environments to run directly on top of the hardware, without requiring a complete host operating system.

Application virtualization – Application is provided to the end user, generally from a remote location (such as a central server), without needing to completely install this application on the user's local system.

Desktop virtualization – Provides the end user with a desktop environment that in turn allows access to any authorized application, regardless of where the appli-



The left part of the figure shows how a traditional architecture has one application running on one set of operating system (OS) and hardware. The virtualized architecture shows a set of applications and OS bundles ("virtual machine") sharing existing hardware using virtualization software.

(Continued on page 2)

A VA Executive's Guide to Virtualization, cont'd

cation is located.

Storage virtualization – Provides a way for many users or applications to access storage without being concerned with where or how that storage is physically located or managed.

Data virtualization – Abstracts sources of individual data items and provides a common data access layer for different data access methods.

WHAT IS THE IMPORTANT TERMINOLOGY I SHOULD KNOW?

Virtual Machine – The software implementation that emulates a physical computer and remains independent of the OS and hardware that host it.

Hypervisor – The software that decouples the OS and applications from the physical hardware. It runs the virtual machines in a virtualized environment.

Software-as-a-Service – Implementation of virtualization where software is provided by an external application service provider. Example: Microsoft Office 365.

Infrastructure-as-a-Service – Highly automated service offering where resources, storage, and networking capabilities are hosted by an external provider. Example: Voice over IP (VoIP).

Platform-as-a-Service – External provider offers operating system, programming language execution environment, database, and web server. Used by application developers to develop and run software solutions on a cloud platform. Example: Google App Engine.

Automated provisioning – Enables self-service for users to gain access to a fully-

provisioned suite of computing services on demand.

WHAT CAN VIRTUALIZATION DO FOR ME?

- Extend the life of older client software
- Reduce capital expenditures and operating costs
- Provide access to systems for workforce (e.g., telework, disaster recovery)
- Increase flexibility to move files around, to encapsulate solutions, to archive, and to optimize
- Reduce reliance and inability to change hardware vendors

WHAT SHOULD I BE AWARE OF WHEN CONSIDERING A VIRTUALIZATION SOLUTION?

Virtualization has revolutionized the way the IT world works and thinks. While this has spurred a lot of innovation or maximized resource potential, the industry is still catching up to itself in some areas. Despite many ready-made and out of the box offerings on the market, the newness of some of these IT tools requires more rigorous analysis and planning before making investment decisions. For an organization like VA, there are two important areas to consider when assessing virtualization or cloud computing: Information Security and Business Process Improvement.

Security in a Virtualized Environment

In comparison with traditional physical computing environments, virtualization can offer significant gains in information security and stronger mitigation of longstanding security threats. With the right tools, your networks will have greater business continuity, more accu-

rate incident reporting, and automated security policies.

Securing information in a virtualized environment poses new challenges. Many cyber security branches of IT departments are only set up to monitor physical computing environments. Virtual environments come with different and new threats to information security to which physical security controls simply cannot monitor or respond. Implementing virtualization requires an investment in virtual security tools to help secure the information stored and processed in virtual environments.

Virtualization and Automating Business Processes

VA relies heavily on a number of disparate business processes to deliver health, services, and benefits to Veterans. One process might make sense for a healthcare unit, while another makes greater sense for assisting with education benefits. Because virtualization is most useful when business processes are standardized and automated, senior leaders should be aware of which business units are appropriate candidates for virtualization. If you invest in virtualized environments without evaluating some aspects of your business model and IT operations (e.g., business process reengineering), the benefits of such technologies may be lost as the result of antiquated policies and procedures written for legacy technology.

If you have any questions about virtualization, don't hesitate to ask CTS (askCTS@va.gov) for assistance or more information. Check out earlier CTS Note editions [here](http://vaww.blog.va.gov/oit360) (vaww.blog.va.gov/oit360).