VIRTUALIZING YOUR INFRASTRUCTURE

SEPTEMBER 2020

ITSAP.70.011

Virtualization is a software-based technology used to create software versions of IT systems and services that are traditionally implemented in separate physical hardware. These software versions, or virtual instances, can dramatically increase efficiency and decrease costs; you can use hardware to its full capacity by distributing its capabilities among many different services. Before implementing virtualization software in your organization, you should understand the associated risks and ensure you protect your network, systems, and information.

HOW DOES VIRTUALIZATION WORK?

To run your systems and services virtually, there are three main components: virtual machines, hypervisors, and hardware servers.

VIRTUAL MACHINE

With virtualization, you can run your applications on fewer physical servers. Applications and software run virtually on a simulated computer system called a virtual machine (VM). The VM has all the features of a computer server, without needing the physical hardware attached. The VM is supported by the hypervisor.

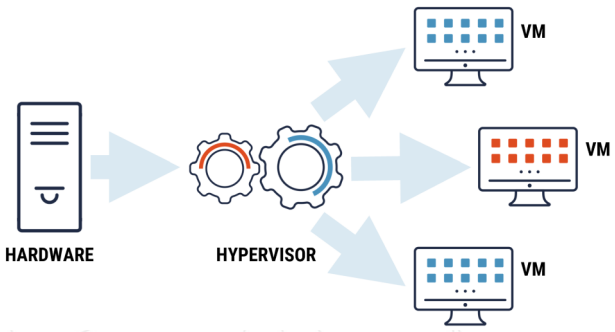
HYPERVISOR

The hypervisor is software that delivers the necessary computing resources (e.g. storage, memory) to multiple VMs, enabling them to run virtually.

There are two types of hypervisors: bare-metal and hosted. A **bare-metal hypervisor** runs directly on physical hardware; a **hosted hypervisor** runs as an application on a host operating system.

HARDWARE SERVERS

A single hardware server may support multiple VMs. Without virtualization, idle applications have resources (e.g. processing power, RAM, storage) that are unused. With virtualization, hardware servers can be used at full capacity to offer the hypervisor all the resources necessary to support the VMs.



WHAT CAN VIRTUALIZATION DO?

Using virtualization, your organization can advance the performance of its infrastructure in the following ways:

- Run multiple operating systems on one physical machine.
- Divide system resources between VMs (e.g. load balance).
- Gain advanced resource controls.
- Create virtualized security appliances (e.g. firewall).
- Move, copy, and save VMs easily to other files and systems.
- Run virtual desktop infrastructure (VDI) in-office and remotely.

For more details on VDI, see *ITSAP.70.111 Using Virtual Desktop At-Home and In-Office* on our website (**cyber.gc.ca**).

WHAT ARE THE BENEFITS?

Virtualization has several benefits, including the following examples:

- Lower costs for high performance IT services.
- Increase IT productivity, efficiency, and responsiveness.
- Offer flexible work arrangements with remote access.
- Accelerate the implementation of applications and resources.
- Minimize network downtime.
- Decrease disaster recovery time.
- Simplify data centre management.
- Segregate applications and data to enhance security and reliability.
- Create environments to safely test applications.

AWARENESS SERIES

WHAT ARE THE RISKS?

Your organization can introduce security vulnerabilities if you do not properly configure or secure virtualization technology. Risks may include the following examples:

- Vulnerabilities can be introduced by obsolete and unpatched servers.
- Sensitive data can be compromised by moving VMs.
- Entry points (e.g. external access to the device) can be exploited when VM is offline and dormant.
- Hardware can be compromised by malware that spreads from VMs or hypervisors (e.g. VM escape).
- Unauthorized access may be permitted due to virtual separation not offering the required isolation for security baselines (e.g. privileged access).
- Loss of control and visibility if traditional security devices are used.
- Resources can be exhausted if a hypervisor is compromised or if unauthorized changes are made to configurations.

HOW DO I SELECT A VENDOR?

You should choose a vendor that can support your organization's security requirements. Before selecting a vendor, ask the following questions to help support your decision:

- Is data encrypted when it is in transit and at rest?
- Does the vendor have security controls in place that can protect sensitive data?
- Does the vendor offer private tenancy (e.g. hosts your data in an independent database) to ensure your organization is not sharing physical hardware with other clients?
- Does the vendor use bare-metal or hosted hypervisors?
- Does the vendor have monitoring and auditing capabilities?
- Who can access the server's data?
- How are administrative privileges controlled?
- Are servers located in Canada (i.e. vendor is subject to Canadian privacy laws)?
- Does the vendor give advice and guidance on configuring, deploying, and hardening the virtualized environment?

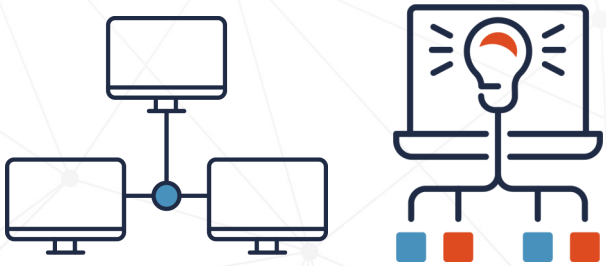
HOW CAN I MITIGATE THE RISKS?

Your organization can mitigate some of the risks associated with implementing virtual technology by taking the following actions:

- Select a trustworthy and reliable vendor.
- Update and patch servers frequently.
- Have your IT team separate the different areas of your virtualized environment (e.g. public, storage, management) into network zones for better control.
- Store highly sensitive data on separate physical servers.
- Test high-risk applications in isolated environments.
- Apply the principle of least privilege to ensure users only have enough privilege to carry out their job functions.
- Use separation of duties to break down processes or tasks into a series of steps to reduce the likelihood of mistakes or malicious activity.
- Use multi-factor authentication for all accounts.
- Train employees on cyber security best practices and provide role-based training (e.g. for administrators).

We strongly recommend using a bare-metal hypervisor for your organization's virtualized environment. A bare-metal hypervisor is built with fewer layers of components, exposing it to fewer vulnerabilities.

For more information on virtualization, refer to *ITSP.70.010 Cyber Centre Data Centre Virtualization Report: Best Practices for Data Centre Virtualization,* which is available on our website.



Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**