What's the difference between a sandbox and a virtual machine?

Ask Leo! by Leo Notenboom

Helping people with computers... one answer at a time.

Ask Leo! » General Computing

Sandboxes and virtual machines share some characteristics, but they are fundamentally different technologies. I'll look at both from a high level.

by Leo A. Notenboom, © 2012

Sandbox versus virtual machine: can you provide a brief overview on the differences, advantages, and disadvantages?

•

Sandboxes and virtual machines are two different technologies that share just enough characteristics to make them easily confused.

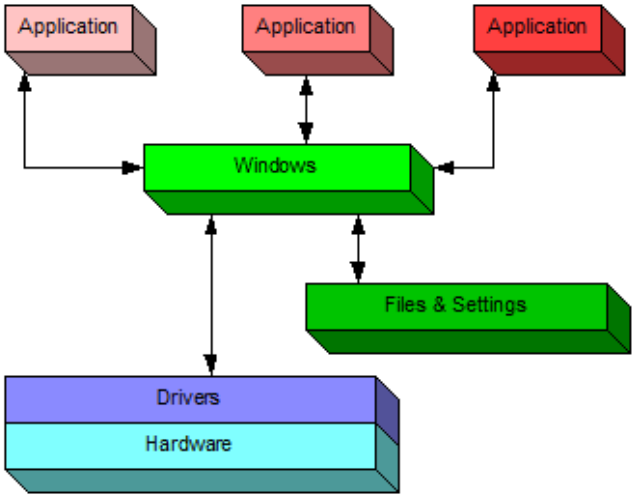
One could even confuse matters further by referring to a virtual machine as the ultimate sandbox. That would be an accurate statement, but it really only stirs up the mud in what is already muddy water without a little background.

Let's look at the three scenarios: the default case without either, a sandbox, and a virtual machine.

•

Windows on its own

Let's start with a conceptual view on how Windows and Windows applications operate at a very high level:

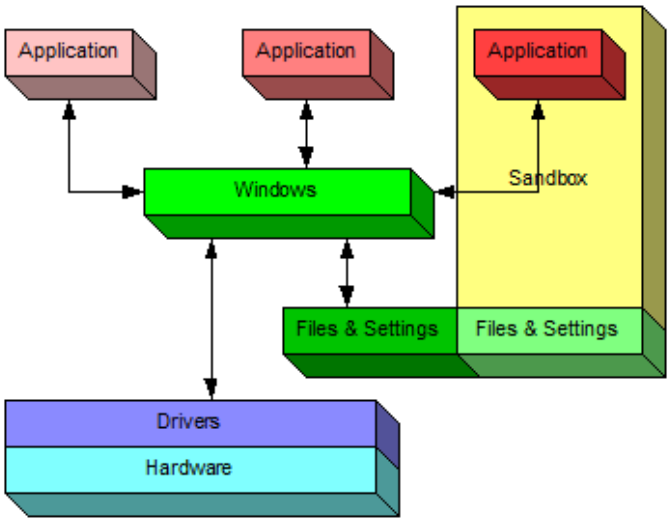


As you can see in the above diagram, applications running in Windows interact with the machine and with you *through* Windows.

Windows manages access to the files and on-disk resources; it also manages access to the hardware through the device drivers that are installed for your machine's specific hardware configuration.

A sandbox under Windows

In a sense, a sandbox is a container placed around an application running within Windows:



You'll note that one of the three applications in this example configuration is drawn as being within a sandbox. Of particular note is that a portion of the "Files & Settings" used by that application are also placed in that sandbox.

Therein lies the magic.

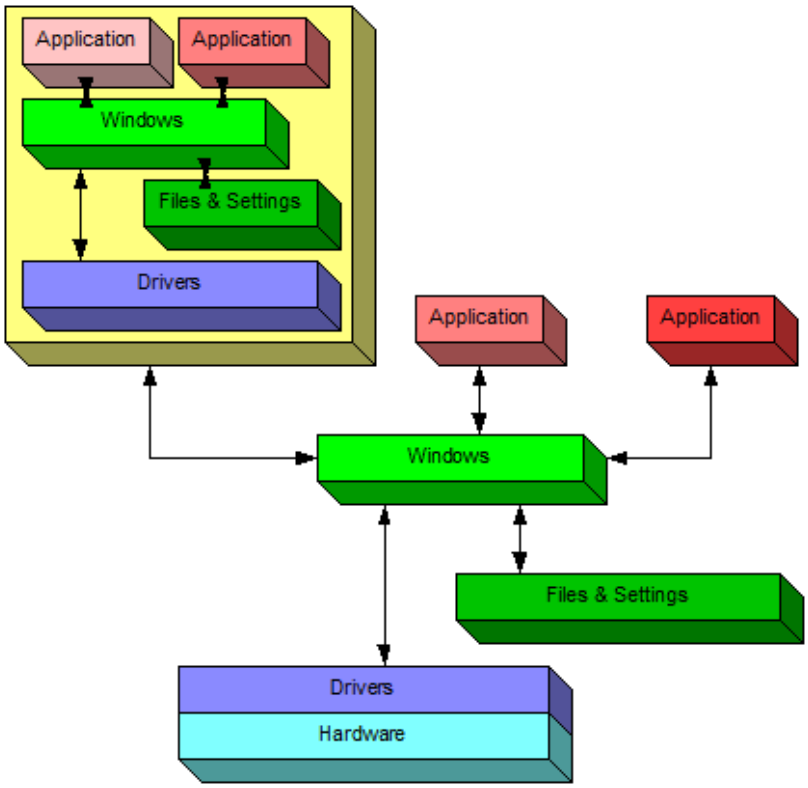
When you run an application within a sandbox, it continues to have access to everything that it would were it not sandboxed. The primary difference is that anything *created or changed* by the sandboxed application is:

- Not visible outside of the sandbox; other Windows applications don't see it.
- Not saved when the sandboxed application exits[1].

The best example is simply that any malware that might have been downloaded and "installed" by the sandboxed application is discarded when the application exits.

A virtual machine under Windows

A virtual machine, or VM, is an application that runs under Windows that creates an environment that simulates a *completely separate computer*.



In this diagram, the application on the left is a VM that's running a completely separate copy of Windows. In a very real sense, it's a "machine within a machine." Windows running on the actual PC is often referred to as the "host" operating system, while any VMs running on it are referred to as "guest" operating systems.

Within a VM, applications continue to access the world around them through that VM's copy of Windows. That "world" includes that VM's own virtual hard disk on which files and settings are stored.

The VM also includes its own set of virtual device drivers that behave *as if* they're interfacing to actual hardware. In reality, they're mimicking the presence of actual hardware and talking to the host copy of Windows to gain access to the real hardware.

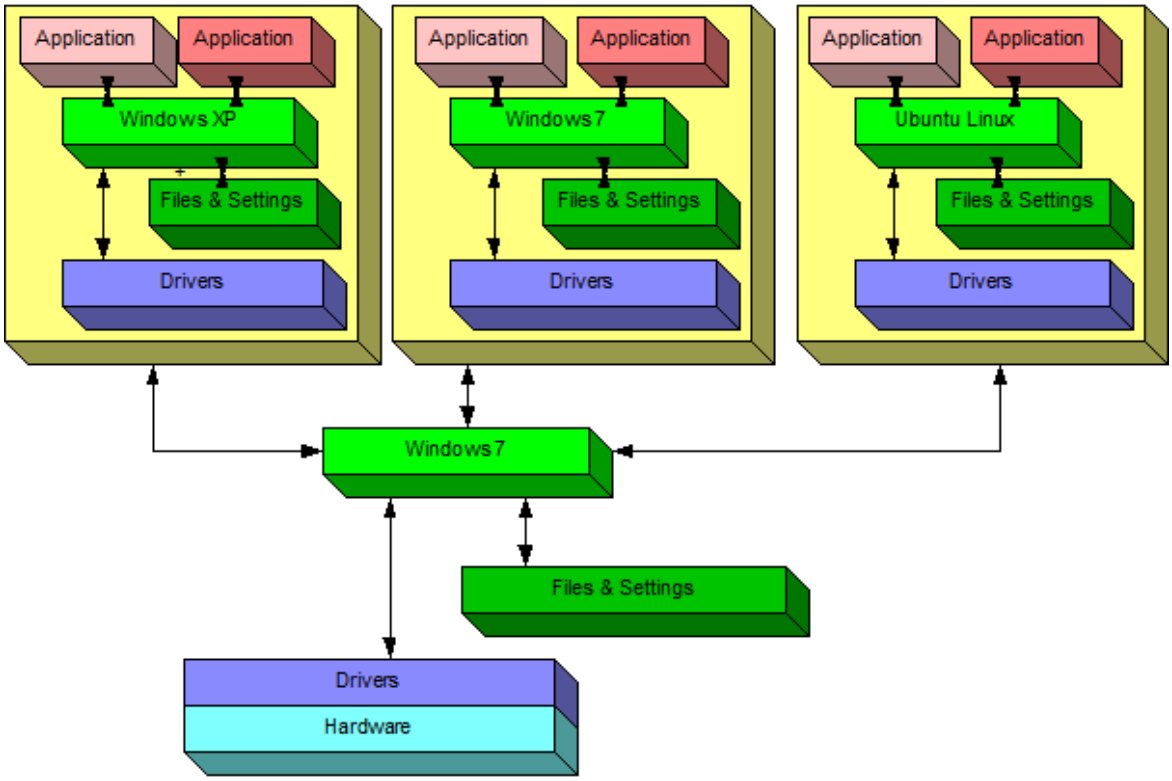
Everything that happens in the VM stays within the VM. It behaves exactly as if it were a completely separate physical machine.

That implies that any downloads, changes, updates, installations ... anything ... that is created or saved within the virtual machine is only accessible through the VM in some way.

And if you delete the VM, it's like getting rid of a PC. Everything on the virtual hard disk is erased.

Multiple virtual machines

One of the best ways to demonstrate virtual machine technology is a scenario such as this one:



This illustrates a single PC running three virtual machines.

- The PC itself is running Windows 7
- One VM is running Windows XP - and would appear as a window within the host Windows 7 machine.
- One VM is running another copy of Windows 7 - and would appear as a window within the host Windows 7 machine.
- One VM is running Ubuntu Linux - and would appear as a window within the host Windows 7 machine.

One physical machine running three different virtual machines simultaneously.

Each virtual machine is completely separate - as if it was on completely separate hardware - except that it's not.

This is actually more common than you might imagine. For example, so-called "cloud servers" are nothing more than virtual machines. As I write this, the Ask Leo! website is in reality a modest virtual machine on a virtual hosting provider. I have no idea what the underlying hardware actually is - the virtual machine can't look "out" to its host. My assumption is that it's a fairly beefy piece of hardware on which several virtual machines are hosted.

Pros and Cons

Sandbox

Sandboxing is typically lightweight and *fairly* easy to set up and use. I say "fairly" because there are complexities, most notably about how to get *desired* changes to be preserved outside of the sandbox.

For example, if your browser is sandboxed (the most common scenario), getting a downloaded file that you want to use outside the sandbox may take a few extra steps. Other changes that you might want to preserve while you're in the sandbox can also be slightly more complicated to retain.

Virtual Machine

Virtual machines are almost certainly not lightweight. You'll need disk space to allocate to the virtual hard drive and you'll also need to make choices about how much of your computer's RAM you want to allocate to the VM while it's running, among other things.

When discussing the characteristics of a virtual machine, the phrase that keeps coming up is "just as if it were a separate physical machine". And when looking at what a VM can and cannot do and what it takes to set one up, that's the best rule of thumb to remember.

Setting up a VM typically involves installing an OS from scratch. In the multiple-VM example above, each virtual machine would need to be set up - just as if they were separate physical machines.

A virtual machine and its host are effectively isolated from each other. A common way to copy files to and from the virtual machine is to set up network access on that machine - just as if it was separate physical machine.

As you can see, a VM is perfect if you want a completely isolated "virtual" second (or third, or fourth) machine. It's also perfect, particularly if you want that machine to run a different operating system than its host. For example, I no longer have a physical machine that has Windows XP installed on it, but I have virtual machines that I can fire up at will on my Windows 7 desktop that provide me with a copy of Windows XP to work with.

In fact, that's all that "XP Mode" on Windows 7 really is - a virtual machine in which Windows XP can run.

Specific Tools

The most popular sandboxing tool by far is called "Sandboxie". Originally developed as a Sandbox for IE (hence the name), it's grown into a powerful and flexible general purpose sandboxing solution.

I use Parallels Workstation for Windows as my virtual machine technology. I regularly run copies of Windows 7, Windows Vista, Windows XP, and Ubuntu Linux in virtual machines for testing, doing demos, and answering your questions. Parallels is perhaps best known for their VM technology that allows you to run Windows on your Mac computers.

VMWare is another popular VM provider. Of note is that there are many pre-configured VMWare "appliances" that you can simply download and run. For example, you can download a ready-to-run VMWare appliance that is Ubuntu Linux without having to go through the steps of actually setting up the operating system.

VirtualBox is another VM alternative that I've only played with briefly, but it's free and appears well supported and quite robust.

Next steps

I plan to dive into Sandboxie in more detail at some point in the future, as it can be a useful tool in your arsenal against malware. You needn't wait; you might consider checking it out.

Virtual machines aren't for everyone. If you know it's what you need and you have the hardware to support it, it's incredibly cool technology.

But it's overkill for most day-to-day usage.

1: Specific sandbox implementations may provide mechanisms to transfer or save data out of the sandbox, but the important concept here is that, unless such steps are taken, any changes made by the sandboxed application are lost.

Article C5040 - January 14, 2012 « »

Leo A. Notenboom has been playing with computers since he was required to take a programming class in 1976. An 18 year career as a programmer at Microsoft soon followed. After "retiring" in 2001, Leo started Ask Leo! in 2003 as a place for answers to common computer and technical questions. More about Leo.

You may also be interested in:

- Virtual Machines - What Are They? Because I use a VM to present in webinars, I figured that it'd be a good time to demonstrate what they are and why they're so cool.
- Does using a virtual machine keep me safer? By running a non-Windows OS within Windows using a virtual machine you can avoid some issues, but only certain types.
- Does a sandbox or virtual machine help protect your privacy? Sandboxes and Virtual Machines can help isolate you from certain types of threats. We'll look at what they are and how they might, or might not, help.
- Does running Windows in a virtual machine protect me from viruses? Virtual machines are powerful tools that used properly can provide a safe and secure sandbox - used improperly they're as vulnerable as anything else.

Can the VM be made to simulate hardware as well? I am a gamer and would love to simulate older pc's with 3dfx cards.

> *In theory, yes, but I've not run into any that allow for it.*
>
> *18-Jan-2012*

I use VMware player and have the Windows 8 previewer running in it, as well as three different Linux distros. One reason to run a virtual machine might be to do online banking in a safe environment. Another is to experiment with different OS's without tying up a computer. This allows you to start from scratch again easily if you mess something up.

I was also going to say that about games not installing with VM as well. I run W7 Ultimate (64 bit) and first got into Virtual Machine when I couldn't get Status Monitor software to work with my Epson printer under W7. The printer works fine, there's just no way to check ink levels or run maintenance with Epson's Status Monitor under W7. Running out of ink mid-task is not the best way to find I need it and ink is too expensive to guess when it's time to replace the cartridges. I tried a couple programs that are supposed to work like Status Monitor but they had problems like changing the order of the colors so I didn't know which was accurate- color name or cartridge location. None of them worked right with some things hanging up endlessly -not locked up or frozen, just appearing to be doing something while nothing was actually happening. So, I tried the Windows XP Virtual Machine set-up Microsoft offers. It allowed me to install the printer and Status Monitor although it only works less than half the time although the printer works fine. I did try to install some older games and while they appeared to install, none would work. The biggest problem was I was unable to get any gaming hardware to work. I tried several joysticks including an ancient Logitech Wingman Force and an older Logitech steering wheel. I could almost hear it laughing with newer hardware like my G27 wheel and Saitek joy stick. Although VM appeared that it was allow installation nothing ever installed. I'm still hoping someday to find a VM program a bit more functional. Until then I am hanging onto my faithful old XP based machine as well for older games. W7 compatibility mode is not as good as you'd expect.

An aside is the term 'Sandbox' also applies in gaming and means a game where you don't have to follow the script constantly and can freely roam about doing (almost) whatever you want. What immediately comes to mind are the Grand Theft Auto games. To a lesser degree are Fallout 3 and Fallout New Vegas.

Oh yeah, and VM DOES require a separate anti-virus. Cheapest way for me was is to get the 3 PC version of my favorite security suite! A number of ISPs offer free brand-name security suites to subscribers. Mine does not limit how many PCs it can be installed on.

Isn't Chrome already using sandbox technology for general browsing? I think I read recently that in Chrome each tab is its own sandbox. Do I have that right? I use SR Ware Iron, which uses Chrome as its core, without all the Google privacy concerns. I have used it for a few years, and I love it. Updates to Chrome are automatically applied to Iron as well.

> *It's not true sandboxing as discussed in this article, or you'd never be able to save a download or make a chrome setting change. Chrome does give each tab its own process which reduces the problems one web page you're viewing might cause to another.*
>
> 
>
> *18-Jan-2012*

Dell has had the Secure Firefox for well over a year now. This provides safe surfing with a built-in sandbox. No configuring is needed.

It is called KACE secure browser and it is free to anyone. Many of my customer's now use it.
Packrat1947

OK, I understand more than I did before about the differences, but does this include the JVM, or Java Virtual Machine?

> *The JVM does use a form of sandboxing, yes, but it's really not related - other than in concept - to what this article is discussing.*
>
> 
>
> *21-Jan-2012*

•

Comments on this entry are closed.

If you have a question, start by using the search box up at the top of the page - there's a *very* good chance that your question has already been answered on Ask Leo!.

If you don't find your answer, head out to http://askleo.com/ask to ask your question.

---

http://ask-leo.com/whats_the_difference_between_a_sandbox_and_a_virtual_machine.html