E-NEWS

Quick Guide to Virtualization as a DR plan

Although many business owners think that Virtualization and Disaster Recovery (DR) are two separate services, the former can actually be used as a legitimate solution to the latter. Here's how it works, along with some pointers to keep in mind should you choose virtualization as your disaster recovery plan.

Unlike tape backups, Virtualization restores your entire system in four hours or less by recovering your backed up servers, operating systems, and applications via the internet. This means you'll lose fewer critical files due to minimal downtime and can resume normal operations promptly.

While the speed of virtualized backups might sound alluring, there are a few key points you should be aware of before moving forward.

- **Backup location for critical data** – Where do you want your critical resources to be stored? Do you want it stored on tapes, disk technologies, or virtualized servers? Even if you choose virtual machines as your main backup plan, it's highly recommended to back up your critical data on multiple sources to lower data loss risks and ensure fast recovery.

- **Data to be backed up** – If you decide to back up your critical data on virtual machines, you should figure out which data you want to store and designate specific virtualized servers to store them. In case a disaster does happen, you'll know immediately where your backups are and can retrieve your data quickly to get your business up and running again fast.

- **Systems to be virtualized** – You should also identify and back up critical applications that's necessary for your business's operations, such as email, Microsoft Office programs, and other in-house applications. Once identified, you should remember to virtualize and store them off-site for seamless disaster recovery when your local servers fail.

If you choose Virtualization as part of your Disaster Recovery solution, make sure your backups are monitored regularly so they're up-to-date in the event of a disaster.

Besides Disaster Recovery, there are many other benefits to Virtualization. Your business can reduce the amount of servers and other hardware in your office, lower electricity expenses, spend less time maintaining on-site servers, and save money in the process. Consider Disaster Recovery as a nice bonus that's included with these benefits.

Curious to learn how else Virtualization can benefit your business? Interested in a dedicated Disaster Recovery solution? Call us today and discover how our experts can protect your organization and save you money.

Virtualization security risks & management

While virtualization security is often viewed as an afterthought, it is nevertheless important. Like all technology, securing your virtualized infrastructure is vital to your business's success. Let's take a look at some of the security risks posed by virtualization and how you can manage them.

Security risks of virtualization

Complex infrastructure – Much like virtualization itself, the infrastructure of a virtualization solution can oftentimes be confusing to small businesses. In fact, the complex configuration alone can be a big headache for it's more difficult to spot anomalies and unusual events happening in your virtual machines and network.

Dynamic design – Virtualized environments are dynamic by nature and constantly changing. Unlike adding physical equipment, the addition of virtual machines can go almost completely unnoticed as they're created in a matter of minutes and aren't visible in your workspace. The danger here is the age old adage, "out of sight out of mind." And if you add too many, they can easily become difficult to manage and protect, creating security holes in the process.

Quick moving workloads – As your virtualized infrastructure grows, there will come a time when you need to move data from one machine to another. While this may sound harmless, the real issue is that your virtual machines will likely require different levels of security. And when you're juggling multiple workloads over multiple virtual machines, you may accidentally move mission critical data to a machine that has minimal protection.

How to mitigate risks

While these three risks may sound alarming, they can all be mitigated. The key behind effectively securing your virtual machines all comes down to process. Put some thought into your security processes and then implement them. Here are a few areas to cover:

- **Organization** – Decide how and where to separate your test, development, and production virtual machines.
- **Audit** – Develop a system to regularly audit your virtual machine security. Whenever possible, use tools to automate your security checks, balances, and processes.
- **Patches** – Perform regular security maintenance to ensure the patches are up-to-date for all virtual machines.
- **Overflow management** – Create a system to monitor all your virtual machines, identify what each of them is used for, and manage them accordingly.

- **Responsibility** – Designate an IT technician to watch over your virtual machines to ensure zero security gaps.If you prioritize proper management of your virtual machines, security doesn't have to be an issue. Get in touch with us if you're interested in getting additional assistance for your virtualized infrastructure or if you're planning to implement a new virtualization solution. Call us today!

E-Safe Technologies Lab Day!

Join E-Safe Technologies **Thursday, September 13th** and work with our experts on Virtualization through VMware!

REGISTER HERE

Topics to be covered:

- **VMworld 2018 updates, overview and recap**
- **Advanced logging and troubleshooting within VMware**
- **Using host profiles to back up you ESXi host configurations**

IMPORTANT NOTE*
vSphere 5.5 is End of Support on September 19th!
An upgrade off of vSphere 5.5 is ESSENTIAL!

Be sure to register today!

Let's talk security at our exclusive event at Top Golf!

You're invited!

Join us and our co-host, **Barracuda**, for some fun at TopGolf! Enjoy food, drinks and golf all on us!

Plus, see how easy it is to protect Office 365 email and data from advanced threats with Barracuda Essentials, a complete and affordable solution for email security, backup, archiving and eDiscovery.

Don't miss this fun, free and informative event!

Save your spot – right now.

To register visit:

https://www.barracuda.com/events/registration/1535558573

Overview

Date: September 27, 2018

Time: 12:00 PM - 4:00 PM (EDT)

Location: Top Golf
400 Presto-Sygan Rd
Bridgeville, PA

4 tips to speed up your Windows 10 computer for free

If your Windows 10 computer is starting to slow down after some time, there are ways to make it run faster without breaking the bank. The following tips will improve your computer's performance without the need for more hardware.

Prevent programs from launching at startup
Windows loads several programs at startup so they're quickly available. While Microsoft likely has good intentions for doing this, the auto-launch can also slow down the speed of your computer. To fix this issue, you'll need to make some manual adjustments in the settings.

To see what programs launch during startup, press Ctrl+Shift+Esc. Next, click on the startup tab of the "Task Manager" window, where you can easily disable any programs you don't want launching at startup. However, there will likely be a few programs you're unsure about. For those, it's best to play it safe and keep them enabled.

Get rid of useless applications
Having too many programs on your computer take up valuable memory and hard disk space. They slow your computer down and make it work harder than necessary. To quickly clean out your unused programs, follow these steps:

Tidy up your disks
While most people like to clean out their houses come spring, why not do so with your computer sometime this month? Thankfully, Microsoft's Disk Cleaner tool makes it easy to do so.

To find Disk Cleaner, right-click any drive in File Explorer and select "Properties" and "Disk Cleanup" under the "General" tab. Once open, it will automatically find files that may be taking up unnecessary space, such as temporary Internet and system memory dump files, and present them to you for your review. Once you've looked them over, you can easily erase them by simply clicking "OK".

Turn off apps running in the background
Much to your surprise, there are likely some programs running in the background of your Windows 10 OS that you're completely unaware of. Microsoft has enabled their native universal apps to do this so you can quickly access their features. However, it also will slow down your CPU, so you might want to disable them.

To find out what programs are running in the background, navigate to "Start Menu>Settings>Privacy>Background" apps. Then, switch off the programs you don't want running at all times.

By following these four steps, you'll see a noticeable difference in the speed of your PC. If you'd like to learn more about how to optimize your Windows system or need assistance with your other Microsoft products, feel free to give us a call.