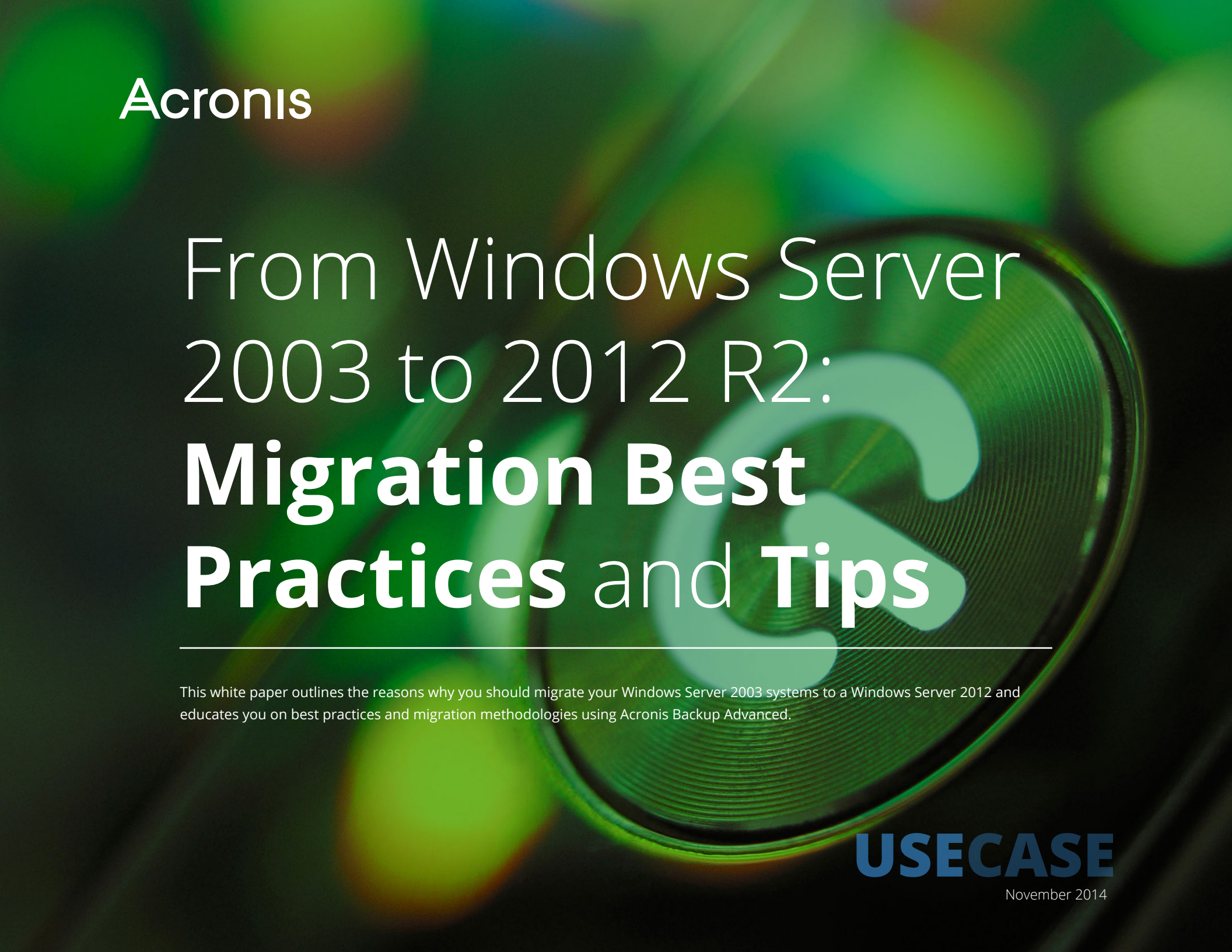


Acronis

From Windows Server 2003 to 2012 R2: **Migration Best Practices** and **Tips**

This white paper outlines the reasons why you should migrate your Windows Server 2003 systems to a Windows Server 2012 and educates you on best practices and migration methodologies using Acronis Backup Advanced.

USECASE

November 2014

Why Should I Migrate from Windows Server 2003?

Since its launch on May 28, 2003, Windows Server 2003 has become the backbone of data center operations and one of most popular Windows Server operating systems ever. Twenty-three million servers worldwide still use Windows Server 2003. According to W3Techs, 31 percent of the Windows-based web servers still run IIS 6.0, on Windows Server 2003. Now after almost 12 years, Microsoft will discontinue Windows Server 2003 support on July 14, 2015.

In the first 6 months of 2014, Microsoft released 27 security bulletins for Windows Server 2003, deeming 12 of them 'critical'. As with Windows XP, governments and large corporations may pay Microsoft® millions of dollars for out-of-band support. If your organization cannot afford the high cost of extended support, it is time to move away from Windows Server 2003. Here are six reasons why you should start planning now.

1. No more technical support

Microsoft will stop releasing patches for Windows Server 2003 on July 14, 2015, which means that Microsoft will no longer address technical issues, usage queries, bugs, and security holes. If your Server 2003 system does not boot or you experience critical errors, there will be no one to call for support. This even applies to enterprise support customers, as Microsoft will automatically exclude Windows Server 2003 from the contract scope. If you run a business with users who are dependent on Windows Server 2003, you are at risk of serious downtime and potential loss of data.

2. No more updates

Microsoft will not provide any future Windows Server 2003 updates, so you can expect that the operating system will not be compatible with future versions of other software applications.

In fact, the latest Microsoft Exchange, SQL, and SharePoint® versions are already incompatible with Windows Server 2003. These incompatibility problems will only become worse over time.

3. No more security patches

"Customers see security fixes as being among the most critical fixes for their installed servers. These fixes will no longer be delivered to customers for their Windows Server 2003 servers, regardless of how severe a given issue may be", **said Al Gillen, Program Vice President, Servers and System Software at IDC**. "This may be less of a problem with many aging Windows Server 2003 applications, mainly because the applications still in use are increasingly likely to be inward facing rather than outward facing."

From a security perspective, this has several implications. First, Microsoft will never make patches available for the dozens of potential security breaches that Microsoft estimates will occur this year.

That means if you continue to use Windows Server 2003, there are numerous backdoors a hacker can use to exploit your systems. Virus infections will become epidemics. Denial of service attacks, advanced persistent threats, zero-day attacks, and SPAM are very real and prevalent dangers.

Furthermore, any vulnerability discovered and patched in Windows Server 2012 R2 has a high likelihood of existing in Windows Server 2003 as well. Malware authors will reverse-engineer these patches to discover how to exploit and attack Windows Server 2003.

With the end of life of Server 2003, one in three Windows web servers are at a higher risk of becoming a victim of hacker attacks.

In addition to the potential downtime, data loss, and brand damage associated with hacker attacks and viruses, your organization can also be in a non-compliant state if you are subject to regulatory requirements such as PCI 3.0 or HIPAA.

4. Fewer drivers

Hardware vendors use Microsoft Windows Driver Kit (WDK) for driver development and the current version (v8.1) of WDK does not support Windows Server 2003. As a result, hardware vendors will need to invest resources and money to develop Server 2003 drivers. This will ultimately result in these vendors discontinuing Server 2003 support.

5. Less application software

The same argument for drivers also applies to application software development. The frameworks, kits, and libraries used by software vendors have minimum operating system requirements. This means that there will be less application software for Windows Server 2003.

6. Move to a virtualized environment

Windows Server 2012 R2 comes with the Hyper-V® role that provides the infrastructure and management tools to create and manage a virtualized environment. This lets you:

- Split workloads that are overcrowding your old 2003 server
- Consolidate workloads to make your new hardware more efficient
- Reduce license, management, maintenance, and utility costs by reducing the number of servers
- Realize immediate payback on a migration project by moving to and leveraging virtualization.

Ensuring Safe Migration

As of July 2014, Microsoft estimates there were approximately 23.8 million instances of Windows Server 2003 running across 11.9 million physical servers worldwide. This represents 39 percent of the entire Windows installed base. At the same time, IDC estimates that Windows Server 2012 installations will reach 29.6 percent of the Windows installed base, overtaking both Windows Server 2003 and Windows Server 2008 by the end of 2015.

While we all loved Windows Server 2003, it is time for change. If you choose to keep your Server 2003 systems, you will need to spend money to keep it secure and continuously manage the chaos and disorder an out-of-date operating system creates. Instead, you can proactively migrate from Server 2003 to 2012 R2. If you choose to migrate, it is critical that you safely migrate your systems to a new operating system. Your first step is to assess and plan the migration:

- Do not rush into installing your new operating system. If you do, it is likely that something will go wrong and you will lose your data.
- Determine if your new operating system will run on your existing hardware. Are the drivers you need available? Will your applications run on the new operating system? Do your research and be sure you answer all pertinent questions on software and hardware compatibility as part of your planning process.
- Do not rush into the backup process. Take the time to determine the best backup strategy to meet both your current and future needs.
- Make sure you have a detailed plan. Your Active Directory® and Exchange servers may require different migration scenarios, and even the sequence can be important. Contact Microsoft to the appropriate application vendors to get best practices on how to migrate to new versions.
- Consider performing an initial pilot migration. For example, initially test one to three servers and assess the pilot's success. You can then expand the process to ensure the remaining systems are successfully migrated without affecting your entire business.

How Will I Migrate?

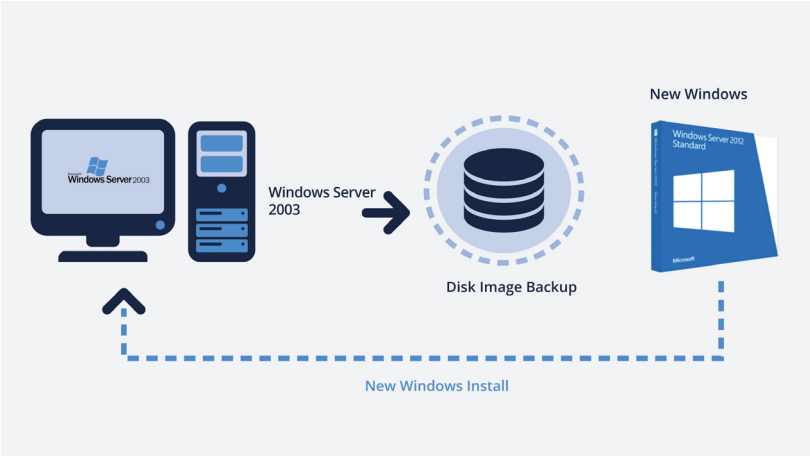
Based on what you discover in the planning stage, your next step is to choose how you will migrate. If your applications and / or newer operating system do not run on your current fleet of servers, you will need to upgrade your hardware. However, if your server is older than three years and you do not have compatibility problems, you may still want to consider replacing them if your budget permits.

You will realize better performance running Windows Server 2012 R2 on newer machines.

On the other hand, if your fleet of servers is new and can run the newer operating system and applications, you can keep the machines and migrate to the new Windows.

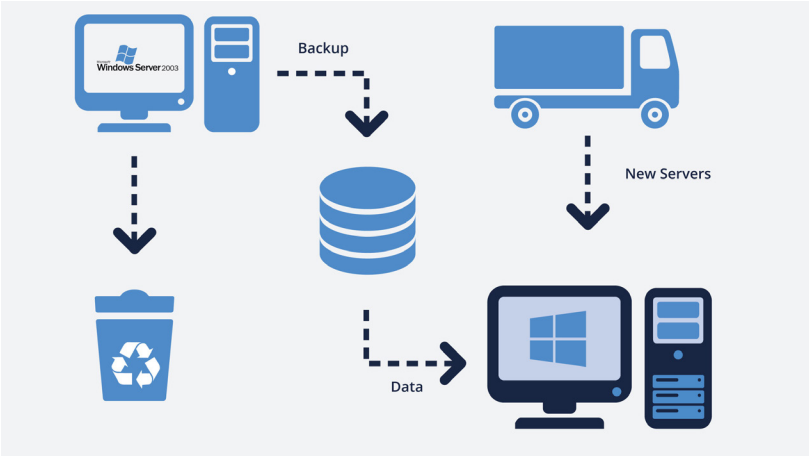
To accommodate these scenarios, there are two ways to migrate: in-place migration (if you plan to keep your hardware) and forklift migration (if you plan to replace your hardware).

In-Place Migration



- Old hardware
- Change operating system

«Forklift» Migration



- New hardware
- New operating system

Migration Challenges and Risks

Data Loss

In either scenario, you can easily make incorrect assumptions and lose data when you migrate from an old environment.

One cause of lost data is that applications save data to a variety of locations in the file system.

Some applications use their installation folders, others use data folders, and still others heavily leverage the system registry.

If you do not preserve everything, you will lose something. The only way to guarantee no data loss during a migration is to use specialized technology designed to save every form of data on the system.

Some applications tie the data in the files to the hardware or license keys. If you back up the file, you must also capture the settings that are required to read the file.

With encrypted files, the key is stored on the system, so backing up only the file does not provide you with the key required to read it.

In short, copying all files is not enough: you will lose data and, in many cases, not realize it until later. You need a way to access the Server 2003 environment even after the hardware is gone and / or the software is migrated to a newer operating system.

Large Effort to Provision

Installing Windows on one machine is easy but what if you have tens or hundreds of servers or more? Deploying software on each can take considerable time and resources. For these reasons, you need a quick way to provision Windows Server 2012 R2 en masse.

Corruption of New Systems

Your new operating system (and hardware) is great, but you need time to become familiar with it. You could inadvertently corrupt the new system, losing data, files, and settings. You need to protect your new systems from data loss and accidental corruption by creating regular backups.

Best Practices for Ensuring A Smooth Migration

Regardless of whether you choose in-place or forklift migration, you need to back up your Server 2003 environment.

You are not doing a simple Windows update – it is a clean install of a new system and the installation process will wipe out everything. If the system is not migrated and restored correctly, your financial data and sensitive company information could be permanently lost, resulting in loss of business, decreased productivity, negative impact on your brand, and more.

It is important that you back up all the information on your Windows Server 2003 machines before the new operating system goes on the drive.

Backup does not have to be a difficult process; you just need to make sure you capture absolutely everything, because you never know what you might need. For most backups, you can use any storage - an external drive or network storage, for example.

Never use the local disks inside your server for backup because the installation process will wipe them clean.

Not all backup and migration solutions are equal. It is easy to make mistakes, so do not be caught in an «oops» moment. Plan and follow these five steps:

1. Back up Your Original Windows Server 2003 Environment

You have used the Windows Server 2003 operating system for years, which means you are storing years of valuable data.

For this reason, you need to back up everything on your old servers. The best way to do this is to use a full backup solution with disk-imaging technology. Acronis invented online disk imaging in 2002 – even before the Windows Server 2003 release! More than 300,000 business customers use Acronis to protect everything on their servers.

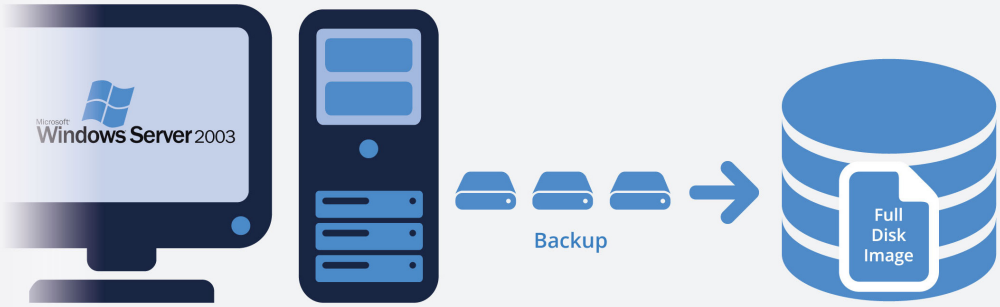
Disk-imaging technology backs up your entire system at the disk level, capturing everything on your system – the documents, data, and user settings – data you may not know that you need. Acronis Backup lets you recover individual files and documents. You can also bring your entire Windows Server 2003 machine back if you ever need it in the future.

You can use any storage: USB drives for one or few machines, or network attached storage (NAS) for larger environment.

If you use a regular file backup solution, or simply copy just the files, you will not be able to bring back the old system, applications, or any specific information that you may need in the future.

Data is not located just in the files but in the registry and hidden partitions. You might also have encrypted data or data stored in a proprietary format. For example, your application serial key may be accessible only from the help menu. How do you get to it after you migrate?

Backup Original Windows Server 2003 Machine on Disk-Level



Backup: Best Practices and Tips

- Use disk-level backup instead of file-level. You can still restore single files or folders, and you can be sure that nothing gets lost.
- Back up all partitions, including hidden partitions. This will allow you to convert your backup to a VM, or easily restore it to a physical machine. If you back up selected partitions, you may complicate virtualization and recovery.
- Back up offline. Offline backup using Acronis backup bootable media ensures that everything you have is safe and no applications are active.
- If you cannot do offline backup (for example, you have 100 servers to migrate), back up during off-peak hours (e.g., after business hours) and then shut down the machine using a post-backup script with the 'shutdown /s' command.
- Back up after the last shutdown. Back up at the last possible moment, right after your final shutdown. Keep in mind that your employees are constantly creating and editing data and files. If you back up your servers the day before migration, you will lose an entire day's worth of data, so create the last backup at the last possible moment before migration. Some organizations trigger backups on shutdown. That helps ensure you have captured the final state. If you do not have the time to do a full backup at the last possible moment, you can run a differential backup to save the most recent data created on your systems, and restore that with the latest full backup. You can also schedule the backup. Lastly, validate all your backups.
- Do not worry about excessive use of storage space. Acronis will not back up free or unused space on the disk, and the software compresses everything you back up.
- Make sure you have the installation disks and drivers for all of your applications. It is a good idea to copy your installation media onto a disk drive to make network installation easier, especially if your new hardware does not have a CD / DVD drive. While you can easily restore your application data from your backup, it is much easier to install your applications from their specific installation media.
- Once you restore your data, do not delete backups. Just because you have switched over to the new operating system does not mean you no longer need the Server 2003 backups. Store all of your backups in multiple locations and on multiple media - an external hard drive, in the cloud, on tapes. Whatever you do, do not delete your Server 2003 backups!
- Your Acronis license is transferable and you can continue using Acronis Backup on your new Windows machines.

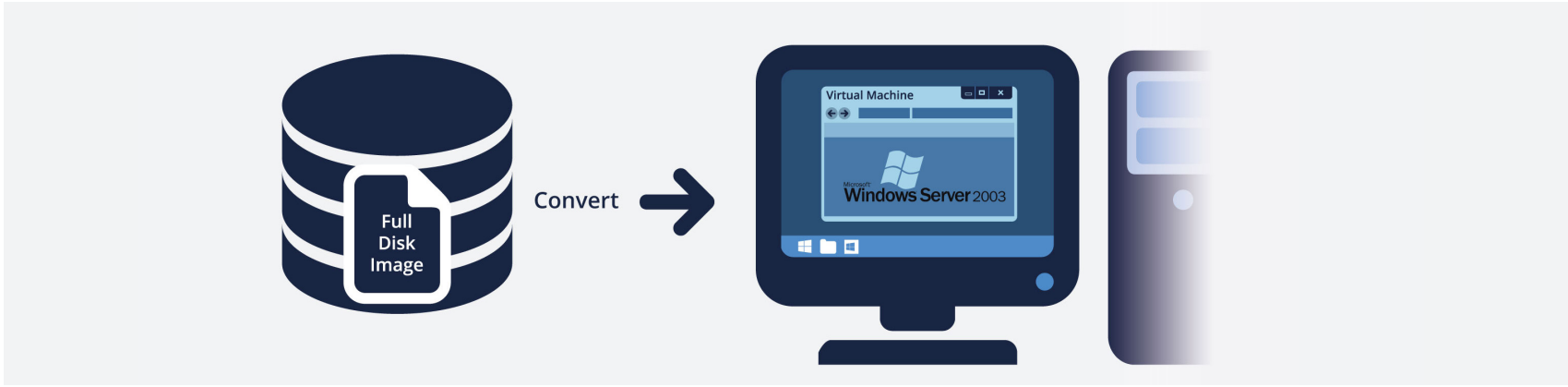
2. Convert the Backup to A Standby Virtual Machine

The server that held Windows Server 2003 may be gone, but the Server 2003 environment can live on. Acronis Backup lets you convert the Server 2003 image to many types of virtual machines, including Microsoft Hyper-V. This is a great way to access your Server 2003 system after migration, and makes it easy to find files and check settings and applications. For example, if after migration you cannot find the serial number for an application, you merely start up the virtual machine and use 'Help->About' to identify the number to use for installation in the new Windows version.

Converting to VM: Best Practices and Tips

1. Convert the VM to the software format that you know best. As your new Windows Server 2012 R2 supports Hyper-V role, the obvious and most popular choice is to leverage this new functionality. However, it is not the only option. If you have experience with VMware® Workstation or Player, use it. If your environment has VMware vSphere®, Acronis Backup supports that too. If you use software that you are familiar with, you will save time when restoring data and settings.
2. Disconnect the network. Before starting the VM, ensure the network adapter is either removed or set to 'not connect' when powering on. By doing this, applications on the VM machine will not conflict with production data.
3. Test-drive a sampling of machines. Do not convert all your machines at once. Convert one or two machines to test and make sure you are comfortable with the process.

Convert the Backup to Standby VM for Future Reference



3. Deploy the New Windows Environment

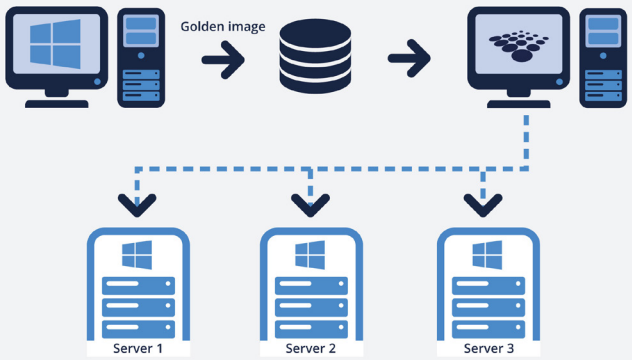
Once the backup is complete, you are ready to deploy the new Windows Server 2012 R2 environment. You can use the standard installation, but that will take a considerable amount of time, especially if you have tens or hundreds of servers. Acronis Snap Deploy® reduces the time it takes to deploy new machines. It is a mass deployment tool that lets you create a master image of a standard machine – including all the applications and settings - and deploy the image to numerous servers via multicast.

Deploy New Microsoft Windows with Acronis Snap Deploy

- Create the master or golden image containing the operating system and base applications.
- Reduce IT administrator's learning curve, improving their focus on the primary task.
- Deploy one machine in the same amount of time as 100 machines, as multicast sends the same image to any number of machines at the same time.
- Be ready in no time, as Acronis Snap Deploy takes care of machine names, IP addresses, domain membership and other settings.
- Save time and eliminate the need to manually boot remote machines from CDs with built-in self-configurable PXE Server for network boot.
- Perform unattended deployment after business hours with Wake-On-LAN.

Deployment Best Practices and Tips

1. Do not forget to back up first. Bare-metal deployment will overwrite everything you have. Do not rush into deployment until you are sure the data is safe.
2. Run a pilot. Deploy 3-5 servers in a first batch and release them to your IT team. You may find applications or settings missing and may need to remake the master image. Re-deploying three to five machines is easier than re-deploying tens or hundreds.
3. Maintain multiple copies of the master image: There may be times when you need more than one master image to accommodate your IT team and users. Be ready with a few master images.



4. Migrate Your Data

Your applications and services may require a special migration approach.

For example, Active Directory requires a rollout on Windows Server 2012 R2 domain controllers, reconfiguration of the domain, and decommissioning of the Windows Server 2003 domain controllers. Your Exchange servers may need to run alongside each other for mailboxes to be migrated.

In any case, consult your application vendor about best practices for migrating data. If you are only migrating files or data for generic applications that do not require a special approach, you can leverage Acronis Backup Advanced, which offers multiple ways of restoring data from your image backups:

- You can mount the backup as a virtual drive in your system and 'copy-paste' files
- You can find specific files in a searchable catalog
- You can use Windows Explorer to navigate inside the backup image and drag-and-drop files
- You can use the Recovery Wizard to easily select specific files that you need

Restoring Data: Best Practices and Tips

1. A successful restore starts with the backup. Use disk-imaging technology to create your backups. You can then restore individual documents, files, applications, or the whole system.
2. Use best practices from the application vendor – all major vendors have precise instructions on migrating data to the newest versions of their applications. You may also consider using trained and certified consultants.
3. Do not try to restore 100 percent of the data from your Server 2003 system immediately – 95 percent is good enough to start. You will never find all the files stored by the applications, so restore as much as you can. When files are missing, IT can retrieve them on an 'as needed' basis.
4. Use catalog search for daily restores and local recovery when looking for ad-hoc files and data. Acronis Backup Advanced provides you with multiple options, so choose the best method depending on the situation.

Restore Data from the Backups

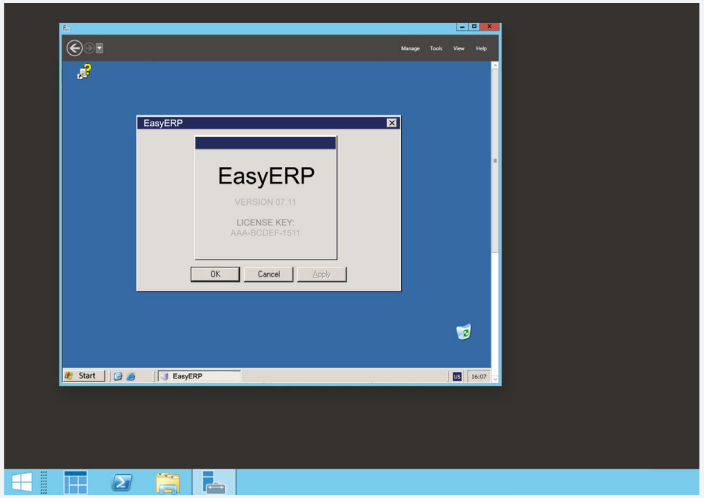
5. Know When to Use the Virtual Machine

You can find any data that is not in a simple file by running the VM you converted from the Server 2003 backup. Application settings, serial keys, proprietary and encrypted data – you can retrieve all of these from the Server 2003 VM.

Using the VM: Best Practices and Tips

1. Use VM-level recovery as a last resort. It is easier to find files and data using catalog-based recovery with search, or mounting and exploring versus launching the VM. If you are looking for just one file, try file-based methods first.
2. Keep the VM disconnected from the production network as much as possible. If you find the file you need, use catalog and search to restore it or 'copy-paste' settings from the VM to the production machine. Use a virtual flash drive to copy output, reports, or settings files. Keep in mind that the VM can conflict with your production machine, so always make sure your users work on the production machine.
3. Use a host-only network if networking is unavoidable. Let the VM talk to only your virtualization host, not the production machines on your network. This way, you can copy files and shield your production machines at the same time.

Restore Settings by Running the Virtual Machine



Summary

Unfortunately, all operating systems meet their end of life. Many times it is better to migrate to the newer operating systems sooner rather than later. When you migrate, be sure to plan, be prepared, do your research, and use the right set of tools to make the migration process as smooth and reliable as possible.

- Back up your Windows Server 2003 environment before you do anything. Acronis Backup Advanced can back up your Windows Server 2003 machines: all the data, files, folders, documents, and everything else you need.
- Once you recover the Server 2003 environment, do not discard your Server 2003 backups. You never know when you may need them.
- Use tools to help you efficiently and reliably provision new machines in your environment. Acronis Snap Deploy can help you to provision your new operating system environment and software to many machines in one step.
- Restore your data and files from your Windows Server 2003 backups. With Acronis Backup Advanced, you can recover any data from your Server 2003: files, folders, and applications. You can even run your old Windows Server 2003 environment as a virtual machine to get anything you need in the future.

Top Reasons to Choose Acronis for Windows Server 2003 Migration

- Capture everything quickly on your Windows Server 2003 machine with patented image-based backups
- Preserve your Windows Server 2003 environment with Virtualization, even if you plan to reuse the hardware
- Deploy your new operating systems en masse to save time and resources
- Recover individual files, folders, applications or your complete Server 2003 system
- Recover to any hardware or VM

Recommended Links

Acronis Backup for Windows Server
Acronis Backup Advanced for Windows Server
Acronis Snap Deploy

ABOUT ACRONIS

Acronis sets the standard for new generation data protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile.

Founded in 2002, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products were named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com.**
Follow Acronis on Twitter:
http://twitter.com/acronis.

Acronis

For additional information, please visit http://www.acronis.com

To purchase products, please visit http://www.acronis.com/en-us/company/contacts.html#international to find an Acronis office or authorized dealer.