Save time: automate the test of backup files!

Although backup testing is part of Business Continuity, many companies give it a miss and do not test their backups or not often enough.

In this guide we will analyse why such deficiencies exist, what are challenges and consequences have the various backup testing formats and how to automate and simplify it with new available technologies.

NetJapan

Do you test backup files every week / day?

When is the last time you simulated an IT disaster?

When IT technicians do not test their backups, or not often enough, the reasons are:

1. Backup tests take too much time

Going through entire backup testing means reproducing a real IT disaster scenario in order to check IT processes. It requires IT technician time, often hours, which they feel they do not have, letting them dismiss backup tests.

2. Backup tests could impact company productivity

Should simulating an IT failure, cyberattack or other disaster during productive hours take several hours to restore systems and data, it will have disastrous impact on employees' downtime and companies' productivity.

We recommend to operate backup tests out of business hours when unsure of process/results. Alternatively, keep reading and find out how to simulate disaster scenario while working with no impact on anyone's efficiency.

3. My backup solution is very reliable and run backups regularly!

Too many IT professionals believe that implementing a backup solution means they will be safe in case of disaster! Hmmm... let's think again: does subscribing a car insurance mean you are never going to be involved in a car accident?

Are YOU yet aware of the importance of backup testing?

Importance of backup testing: If you do not test properly your backup strategy, how will you know your contingency plan is going to work when a disaster hits? How do you know backups will be restorable in the planned timeline if you do not test it regularly?

Any backup and disaster vendor can tell you how reliable and safe their solution is, but it is your entire responsibility to make sure this is the case, today and tomorrow. It will be your responsibility to restore companies' data and systems should a disaster occur.

4. I receive alerts on backup failure... doesn't it mean I test my backups?

No! There are different levels of verification of backup files and it's important to get educated in their importance and impact. Checking backup are created is different to checking backup consistency, and to checking backup can be restored. This guide does explain it all!

Importance of the different verification and test processes

Backup solution vendors often give one or several backup testing options but a lack of official nomenclature of these features across solutions is making it difficult for IT technicians to really compare them and understand what's really verifies and what's not. We will try to elude it for you.

Backup Tests is not a simple process. It is crucial to understand what's tested and the impact on the possibility to restore data and systems should a disaster strike.

Understand the difference between backup consistency, backup integrity, backup bootability is the key to implement efficient backup testing.

Test BACKUP CREATION
Also known as Backup notification

This term often refers to backup creation.

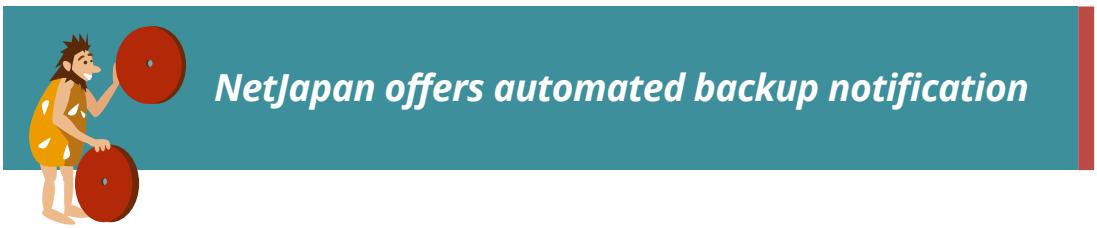
Why activating backup notification?

Set up notification upon backup creation failure to be notified when a backup is not created is the base to any backup test policy. Although you might not be informed of the exact issue, you will at least know you need to investigate to uncover the source of the backup failure. It can be multiple, it can also not be related to the backup solution itself but to a storage device issue, network issue or source machine issue.

It is important to know that notification doesn't check either backup consistency, backup integrity or backup bootability, but it is still important to activate such features you do not want to stay without backups for long.

Backup notification in ActiveImage Protector

Set it up in:
Preferences → Notification



Test BACKUP CONSISTENCY
Often automated process, more or less slow and efficient depending on backup vendors

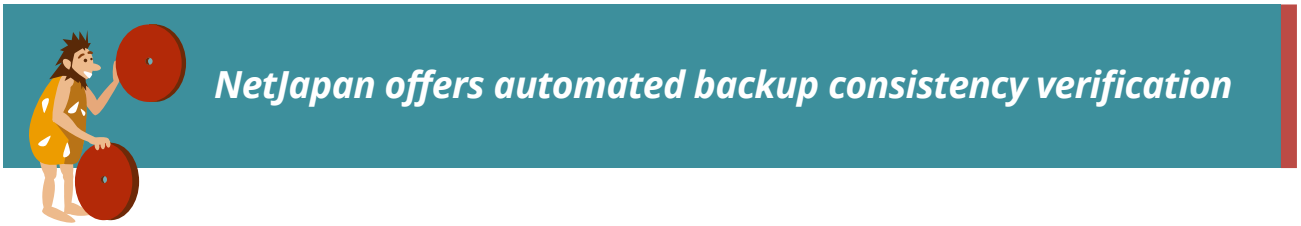
Why backup consistency has become industry standards

Verifying backup consistency: Action of validating backup chain content is readable. Consistent backups can be used or opened.

Backup consistency depends on backup solution reliability as well as storage device behaviour during its lifetime. Indeed, storage device can fail and corrupt or damage incremental backup files from a chain. No point-in-time incremental file dependent on a damaged incremental file can be restored, even if you had initially been notified that backups were successfully created.

Most renowned backup solutions offer backup (consistency verification) as an automated process working in the background. However, such verification tasks can take a long time and use source protected machine resources. Hence a lot of companies choose not to activate it, which we disagree with.

We strongly recommend you to activate this feature!



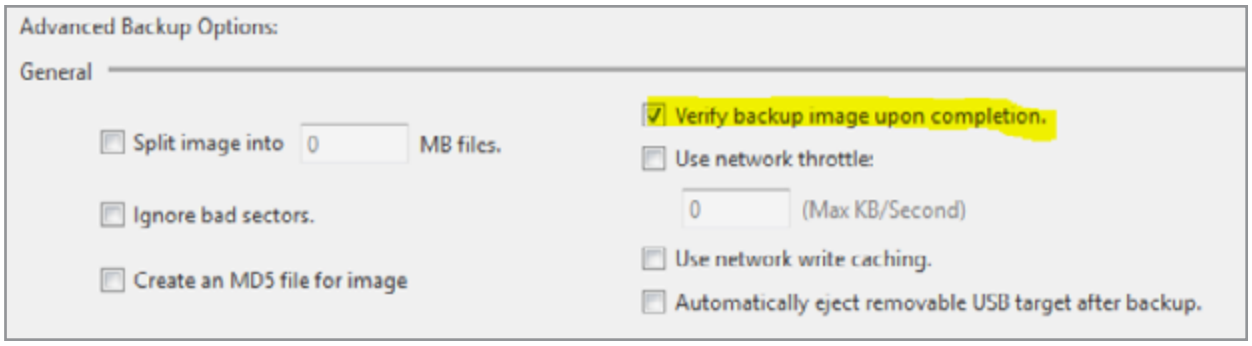
How to setup backup consistency verification in NetJapan solutions

Our backup verification feature checks that each block of each backup file is readable.

You can activate the backup verification feature in 2 different places. It is only necessary to activate it in one of them:

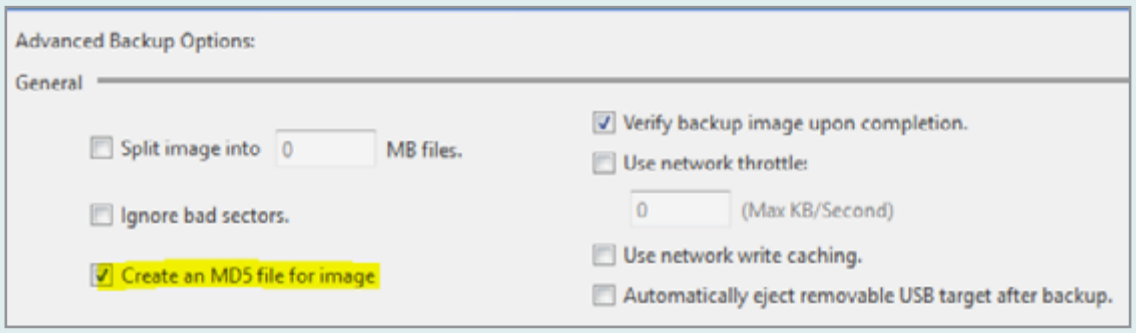
In ActiveImage Protector:

1. Set your incremental backup task and click on “Advanced options” in: Backup task. → 2. Destination
2. Check the box “Verify backup image upon completion”



Notes:

- MD5 checksum:
  It is possible to create MD5 checksum when setting up a backup task in ActiveImage Protector:
  Backup task → 2. Destination → Advanced options → Create a MD5 file for image

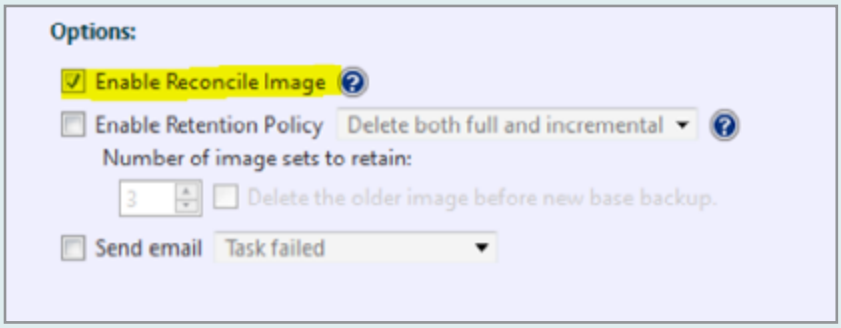


You can use MD5 with 3rd party solutions. However, it is not as reliable as "Verify backup image upon completion" (in the same above screenshot) which we strongly do recommend to activate.

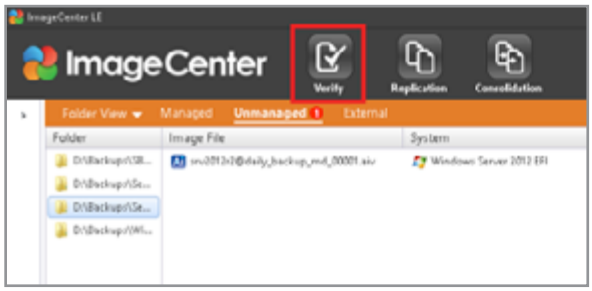
- When creating a backup task containing incremental files, the "Reconcile image" feature is automatically activated, allowing ActiveImage Protector to automatically repair the incremental chain if required. This new auto-repaired incremental file may be bigger to usual incremental files depending on the sector changed since the last valid incremental file. After this one-time automatic self-repair, the incremental backup will continue normally.

  Should you not want to modify the original backup chain (Backup task → 3. Schedule), you can disable "Enable Reconcile Image". In a case of error, a new full backup file will be created (instead of the chain to be repaired).

  Reconcile image feature is found in the backup task, 3rd tab (Schedule), under Options.



In ImageCenter:
Manage your backup chain(s) at "Add image folder" and click on "Verify" to create a task. Follow the easy-to-use wizard, selecting "Sending Email on Task failed" in the Option tab.



Offsite backup consistency

We recommend you to install an instance of ImageCenter (free) at the offsite location and setup the verification process as above.

You can combine it with third party MD5 checksum verification to ensure the copied / replicated data at the offsite location is equal to the source data at the onsite location.

Is backup consistency verification enough for BC backup Test?

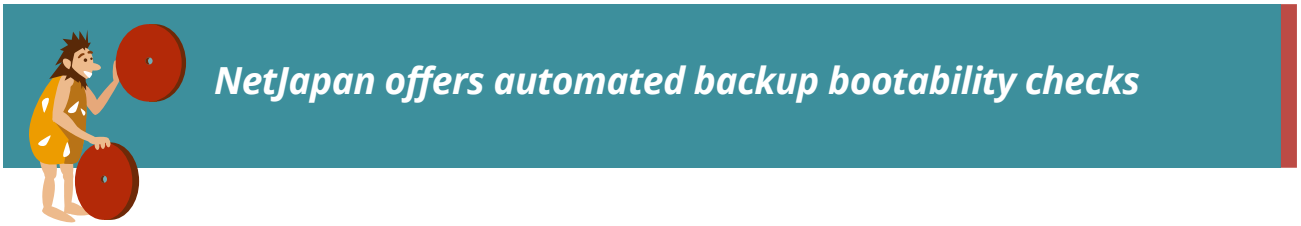
Although it is an essential part of backup testing as part of the Business Continuity cycle, it is not enough. Having a fully readable or fully consistent backup chain does not mean backup chain are restorable!

Consistent backups does not mean either that every single data and file contained in the backup can be used, even when blocks are readable.

Test BACKUP BOOTABILITY
Often the forgotten part of Backup Testing

Ensure no driver glitch or any boot issue will prohibit you from starting your backup file should a disaster strike by testing backup chain "bootability".

Most backup solutions do not provide an easy way to test backup bootability, apart restoring backup files which can be a lengthy process or to operate a manual failover as a VM from backup files. If this second method is often much faster, it still requires IT Technicians intervention and time! NetJapan offers to test backup bootability automatically!



New technology: How does automated backup bootability testing work?

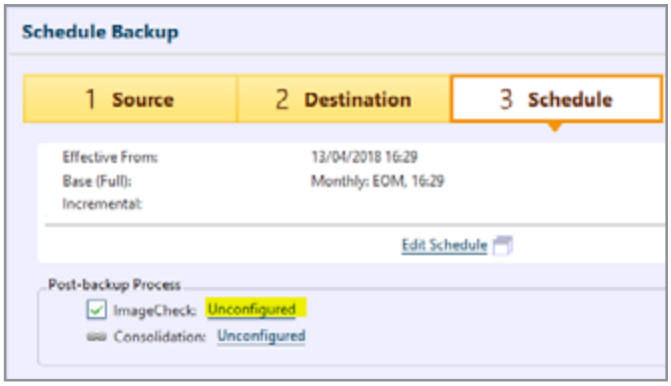
After creation, backup files (full and incremental) are automatically booted as a VM in Microsoft Hyper-V, up to the login details. Upon successful operation, the automatically created VM is deleted. You are notified in case of failure.

For this, you need to enable Microsoft Hyper-V role on the machine that will perform the bootability test. Regardless of their size or length, backups are directly attached as virtual emulated physical disks to the system without any processing time, restore or virtualization task. This fast technology allows us to boot up entire systems and ensure a successfully start of the machine.

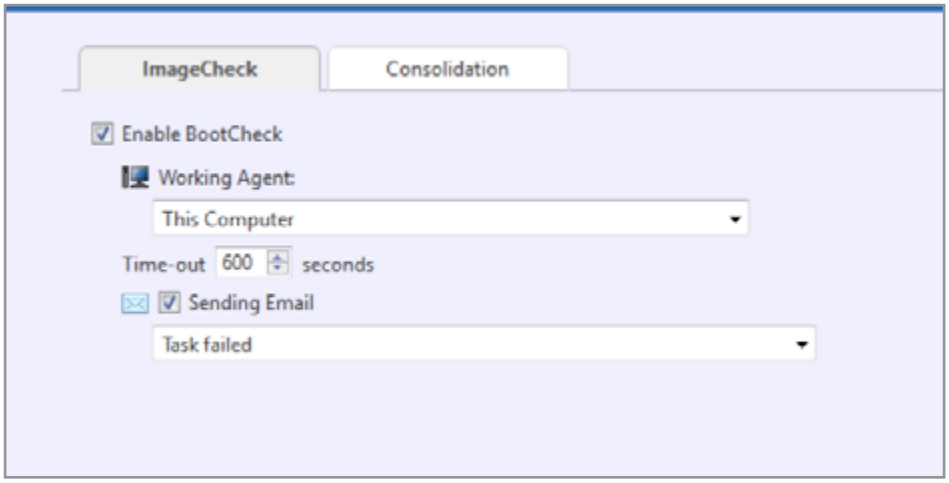
How to set automated BootCheck

In ActiveImage Protector

1. Enable Microsoft Hyper-V (available at Client, Server or Core Windows version) on the protected source machine.
2. Create your backup task in ActiveImage Protector.
3. While setting up your backup tasks, in Backup task → 3. Schedule → ImageCheck, click on "Unconfigured".



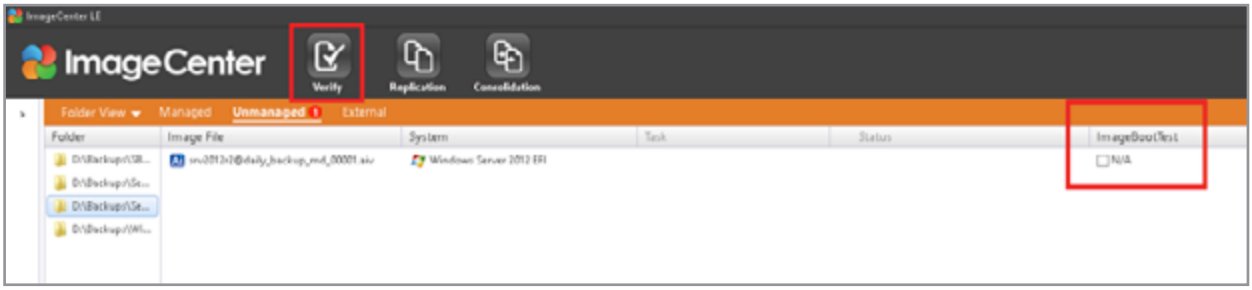
Click on "Enable BootCheck" and configure the notification



If you can't enable Microsoft Hyper-V role on your protected machine, you can use a dedicated system which can use the hypervisor platform and use ImageCenter free add-on as below.

In ImageCenter

1. Enable Microsoft Hyper-V (available at Client, Server or Core Windows version) on the same machine you have installed ImageCenter on.
2. Create your backup task in ActiveImage Protector.
3. In ImageCenter, after having configured image folders, click on the checkbox in the "ImageBootTest" column.



Difference between BootCheck and ImageBootTest?

Both features are exactly the same. Our developers will soon unify the naming.

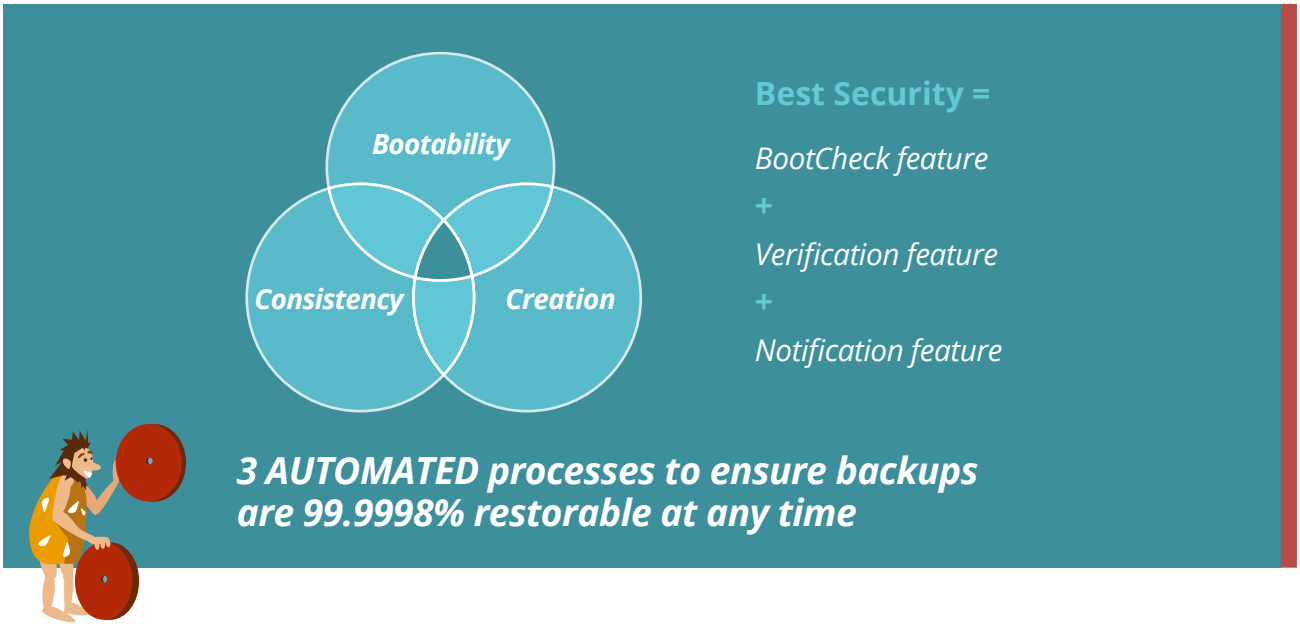
If you do not use ImageCenter replication or consolidation features, or do not use ImageCenter at all, then configure BootCheck directly in ActiveImage Protector.

However, if you do already have an instance of ImageCenter, or plan to use it, then we recommend you to configure automated backup bootability testing in ImageCenter, taking into account our technician recommendations of installing ImageCenter on a separate machine of the network and not on the productive protected machine. The idea is for the protected machine to use its resources for its core activity and not for replication, consolidation or backup testing goals.

Are bootability tests better than consistency tests?

As we saw in this document, both testing processes are different: one tests the system is usable, the other one checks content is readable.

Both are important and both are necessary! You should configure and test all 3 testing parts exposed above. With ActiveImage Protector or ImageCenter, it's simple and it's automated!

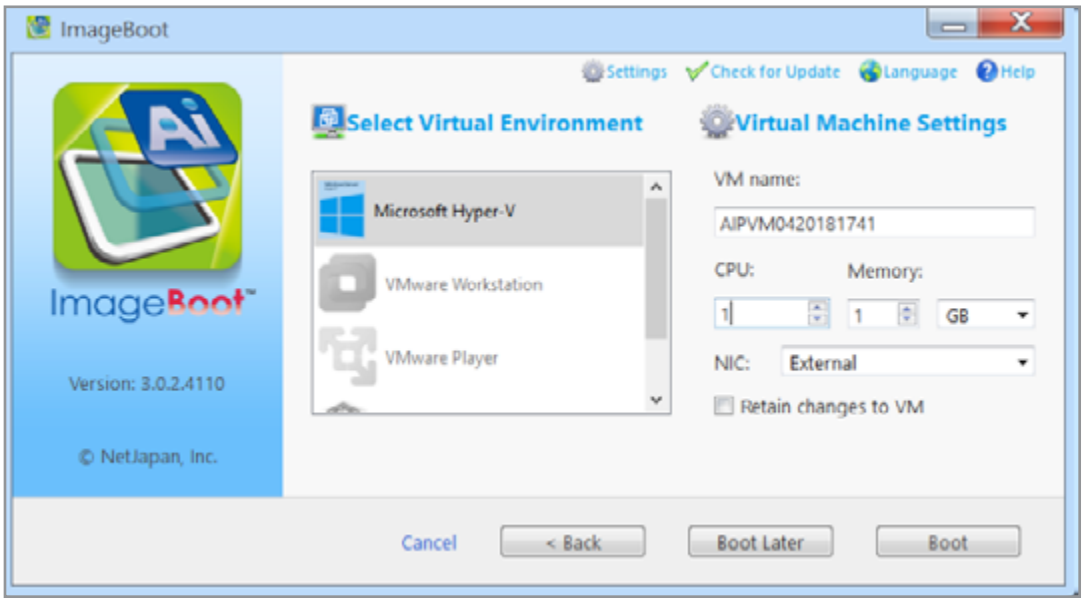


Backup integrity: You will never be better served than by your own eyes

If you are reading this document is that you are in part, or totally responsible for your company's backup file (or your clients backup strategy). The truth is that you cannot be 100% sure but you can get closer by seeing it with your own eyes.

We can help you with it, and it will only take an instant!

Use ImageBoot (free installer included in ActiveImage Protector licences and trials) to boot any ActiveImage Protector backup files in Microsoft Hyper-V, VMware Player/Workstation or Oracle VirtualBox. You will see the selected backup booted as a virtual machine and can even enter the login details to enter. This procedure is instant. It will only take the time for your machine to boot, probably between 2 and 5 minutes.



Once the VM booted, check all data, all applications are there. You can test it all.

We recommend to do this process once a month as it is very fast, but we are sure that if all companies were to do it once every 6 months or even once a year, backup strategies would already progress a lot and would be more successful.

Conclusion

Most companies do not test backup files and that's a mistake.

It is important to first understand the challenges backup tests in order to be able to setup up an effective policy and ensure backups can be restored at any time. For this, technicians need to make sure:

- Backups are created as scheduled
- Backup chains are consistent
- Backups are bootable

NetJapan simplifies IT technician work by offering to test automatically all these 3 aspects.

We go beyond other backup vendors - that offer at best the possibility to test backup creation and consistency automatically – and we provide easy tools to also test backup bootability as an automated process. Backups are safer with our BootCheck function.

Do not hesitate any longer to test it. It's free and included in all NetJapan solutions for physical and virtual Windows machines.

DOWNLOAD A TRIAL