

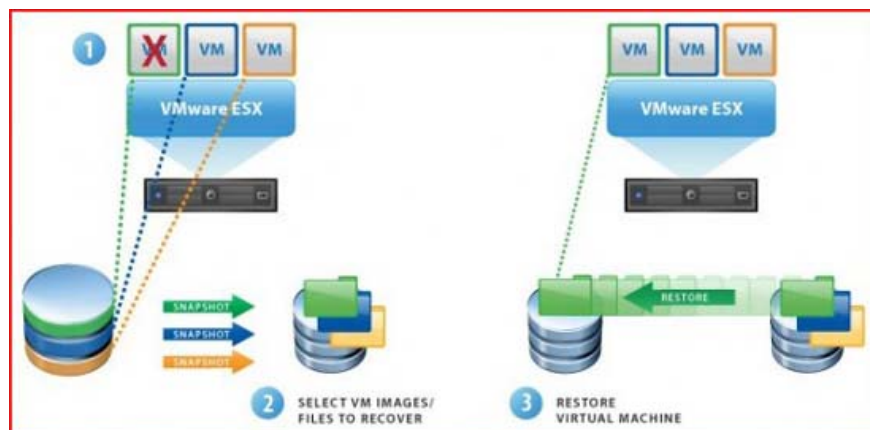
Create and restore backups with VMware vSphere Data Recovery

In this article, I will show you how to create a backup schedule for a virtual machine, run a backup, and then restore the virtual machine from backup.

Network Administration - In our previous introduction to [vSphere Data Recovery](#), we showed you how to deploy DR plug-ins to vSphere4 clients and how to add equipment for virtual infrastructure. chemical. We also introduced one of the key features that is a highly intuitive management interface, integrated with the vSphere client to allow simple configuration of backup jobs. If you have followed the steps introduced in that article, you can now use this management interface to perform some tasks; In this article, I will show you how to create a backup schedule for a virtual machine, run a backup, and then restore the virtual machine from backup.

Basic restoration principles

The vSphere Client Data Recovery plug-in is used to configure Data Recovery virtual machines (DR), virtual machines that recover this data are then used to store backups and perform recovery tasks. In theory, the virtual machines DR can simultaneously backup up to 8 virtual machines, but its CPU performance must be below 90% to be able to perform backup work, otherwise it will wait until it reaches this level. . The process by using the ESX snapshot feature to 'freeze' copy at a time for all disks used on the target virtual machine, this will give it an image. locked for backup while the virtual machine continues to operate, now changes to the disk will be overwritten into a temporary snapshot file.



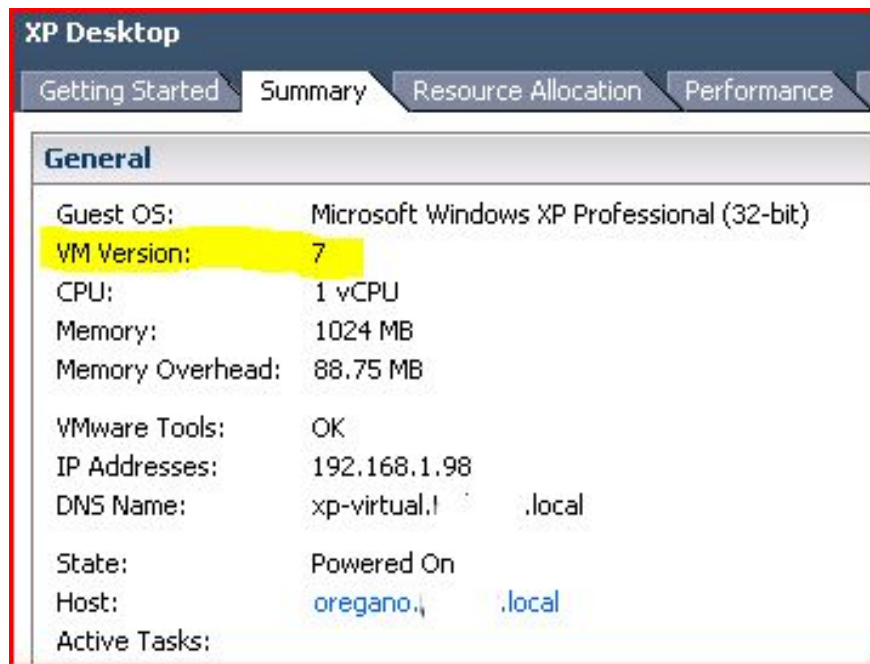
When the backup is complete, the DR virtual machine will release a snapshot to make the disc changes *replay* from the temporary snapshot file to the 'frozen' disk image, bringing it back to a 'live' state.

Data Recovery supports writing backups to certain locations, be it an internal ESX repository or a network address using CIFS file sharing features such as SAMBA or folder sharing in Windows. However, due to memory constraints, only two storage locations can be recorded at the same time, more locations can be

specified, but jobs must be scheduled separately. The limit is that 100 virtual machines can be backed up by a DR VM, although you can create backup jobs more than virtual machines but it will skip. Additional DR virtual machines can be installed to overcome this limitation, but care must be taken to configure backup jobs because the devices may not know each other.

Another important thing to keep in mind to ensure a fully recoverable backup to a virtual machine is to try to create a quiesce snapshot. This requires that the operating system and the applications running on it can write memory-resident data to the disk to be included in the snapshot for the backup, otherwise the applications may lose important data. To accomplish this problem, VMware Tools needs to be installed on another operating system, then Data Recovery will instruct it to perform system quiesce actions during the snapshot process, followed by 'de-quiesce' when the process is completed. With Windows guest operating systems that support Volume Shadowcopy Services, this problem will be handled by the VMware VSP service, otherwise VMware will use any quiesce-enabled features available in the operating system. Therefore, always make sure to install the latest version of VMware Tools on all virtual machines if possible. Failure to install VMware Tools will not stop you from backing up the virtual machine, but the backups will only be 'appropriate accidents' and will require a reboot after a restore.

VSphere 4.0 ESX hosts include multiple **optimizations** for virtual machines that can track virtual disk state changes, but these optimizations are not present on virtual machines created on older versions of ESX (3.5 or older). You can easily check the version you are using on your virtual machines from the Summary tab in the vSphere client:



Virtual machines created on vSphere4 should use version 7, which supports features that enhance data changes and, if created virtual machines on vSphere4 or earlier, they will have version 4 or less. However, you can easily upgrade the VM version, and deserve it, just turn off the VM, then right-click it in the left pane and select "Upgrade Virtual Machine version".



Before doing so, though, make sure you have installed the latest version of VMware Tools on your virtual machines, as the upgrade version also changes some virtual hardware, such as the NIC, into The new driver request section is available in VMware Tools.

This change tracking function allows the Data Recovery VM to analyze changes from previous backups, thus creating many advantages for the backup process. Data Recovery also uses data 'de-duplication' for each storage point, when information is repeated throughout all VM backups, it will only store that information once. This makes the system a significant time saver, especially when virtual machines are running the same operating system and are backed up to the same storage point.

Page 2: Data Recovery setup

Data Recovery settings

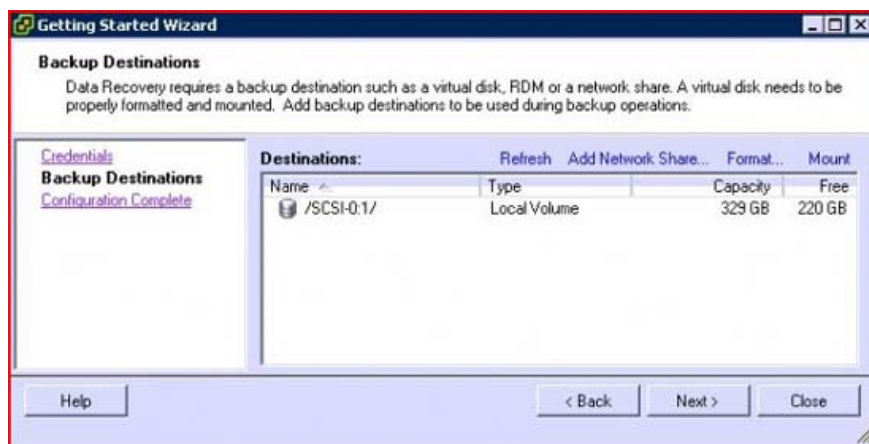
In the previous article, we deployed the VMware Data Recovery device into your vSphere infrastructure, now we need to finish configuring it and creating a backup schedule. Open vSphere Client by navigating to the home page, and you'll see a new icon under the "Solutions and Applications" section for "VMware Data Recovery" - click it to start managing your device. If you don't see the icon appear here, you can review our previous article to learn how to install the management plugin - it must be installed on each vSphere Client system that you intend to use. Because of the release of VMware version 1.1 that has simplified the interface and initial installation process, you can now select your VMware Data Recovery device from the list on the left and click "Connect". The "Getting Started" wizard will then be launched, otherwise, you can launch it by clicking the "

Configuration " tab, then the " **Getting Started** " link.

On the first page, you will be prompted for certificates for the VM-DR device to connect to vCenter Server, depending on the security requirements you can create a separate user account to use. VM-DR devices will initiate some tasks to perform its backups, such as creating snapshots for the VM, so log in with itself so you can easily see what the task is it when checking vCenter records.

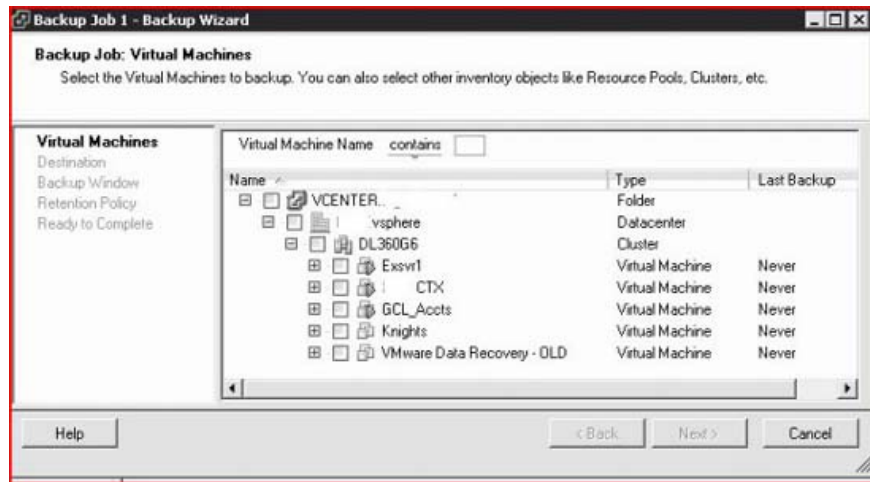
The second step of the wizard is to configure destination storage for backups, with this tutorial, we assume that you are using VMFS storage for your backups, either on the SAN or internal storage, here. are the ones introduced in the previous lesson. However, if you want to use network storage, the process is the same, except that you must click on the " **Add Network Share** " link here and provide the storage point.

Note that VM-DR devices are Linux systems and only support CIFS / SAMBA shares, these shares contain Windows shares but there are some potential problems you may encounter. The first thing to check is that you are using the IP of the target network instead of the name, then if you still have connection problems, we will suggest a search to show you some things you need to check. If you are using VMFS storage, there is nothing to worry about because you will see the disk you added to the device listed in the wizard:

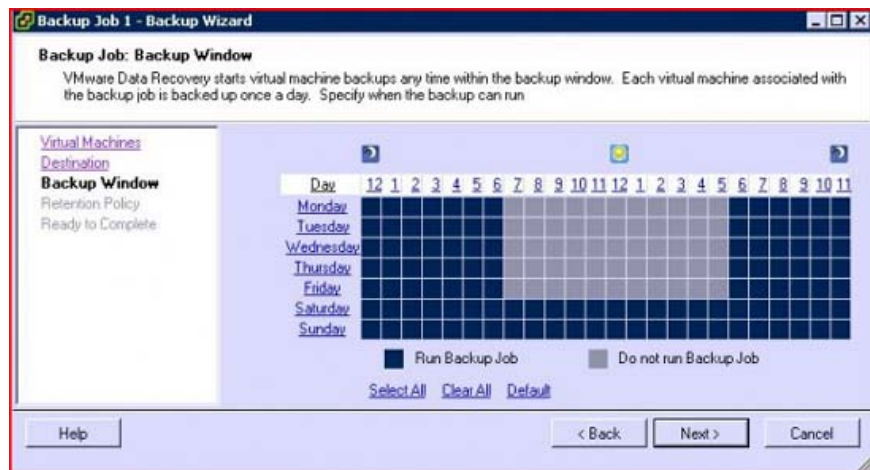


If below "Type" says "unmounted" (not mounted) then you need to click on " **Mount** ", then need the " **Format** " drive, when the process is complete, click " **Next** " and then finish wizard. In the last page, check if you are satisfied with the settings you have selected, check the " **Setup new backup job** " option, then click " **Close** ".

The new backup task wizard will be started, if it does not start, you can launch it by clicking the " **Backup** " tab, then clicking " **New** ". The first page of the wizard will list all virtual machines in the vSpherem infrastructure, with checkboxes so you can select them for your backup process:

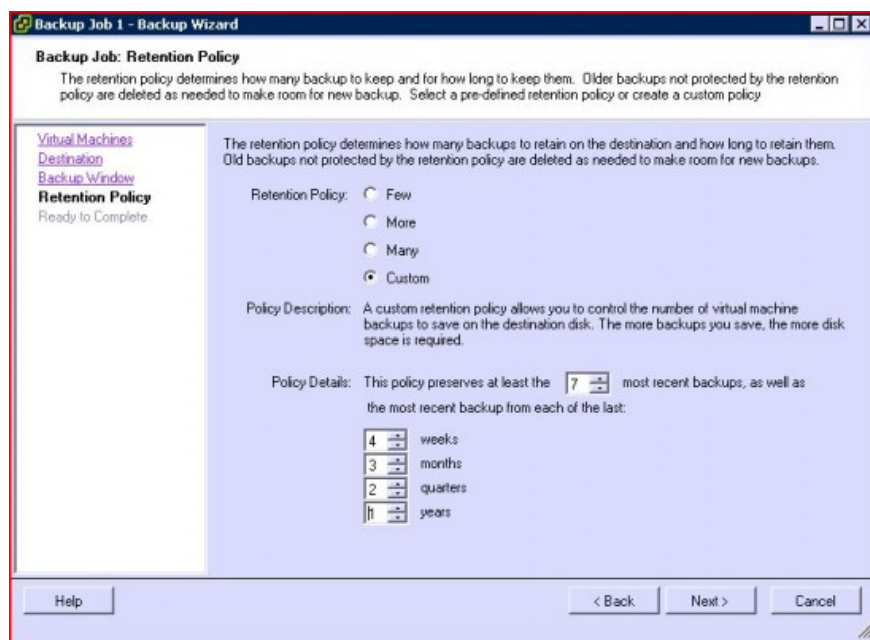


Check the VM checkboxes you want to back up, if you want, you can expand each specific VM, then select certain backup disks, or you can select the cluster / datacenter to back up all the VMs it has include. Click " **Next** ", then on the next page you select the backup archive to save the backups. VMware Data Recovery supports multiple repositories, though it can only backup to two repositories simultaneously.



In the next page, you need to define the 'backup window' (backup window) for the job, as it is allowed to run every day of the week. Virtual machine backups themselves have no effect on performance but the initial "quiesce" operation when the VM is taking a snapshot at an early stage in the backup process can make it "freeze" for a while, especially especially if it has high data throughput. As a result, you need to schedule your 'backup window' so that backups start when users are not online and when requests are processed on virtual machines at the lowest level. In fact, when the initial backup of a VM is complete, the following additional components will be much smaller and therefore completed in a short time, so you can specify a large window to capture. head and then reduce this window later.

There is a limitation of VMware Data Recovery compared to other commercial backup solutions, and you will be limited to the control of your backup schedule. Cannot run multiple backups one day and the exact time of that backup starts to be difficult to control, though usually they will start in the first window every day. You can limit the frequency of backups daily by defining your backup windows appropriately.



In the last page, you must define your retention policy, ie the number of backups you want to keep and how long you want to keep those backups. What you choose here will be a compromise between the amount of storage space and what you need for your backups, as well as the timeline that you can perform the backups needed to restore the system and previous file. At this stage, it is very difficult to give a specific number of the amount of space that each backup will consume, it is a combination of data that is changed daily for archives to be performed. by 'de-duplication'. However, you can choose the policy that is supposed to be conservative ('more' and 'more') now. Then if necessary you can adjust after a few weeks of work. Here you will discover other problems with VM-DR, such as concise reporting, or some other features.

In the end of the wizard will confirm the settings you have selected, so check if these settings are OK or not, then click "Finish" to save the backup job. Depending on whether you are currently in your backup window or not, it may start running the backup job immediately, though in any case, you will see the snapshot export tasks. shown in the task pane at the bottom. The backup jobs themselves do not appear here, but you can check their progress by clicking the " Reports " tab and selecting " Running Tasks ". After a few days of operation, if everything goes well, you will see a list of successful backup tasks on this page, and if you click " Virtual Machines " you will see daily backup points for each VM. .

Practice restoring

It is never a good idea to point out that there is a problem with your backup solution when you need to recover something in a disaster situation, so regular testing is a must. VMware Data Recovery allows you to do this with the " Restore Rehearsal " option, which allows you to restore a virtual machine from a backup without affecting the "live" version itself. It simply runs, just right-click on the virtual machine in the left panel and select " Restore Rehearsal ", then follow the wizard's instructions to restore another copy of the VM to the vSphere data center. When the restore is complete, you can change it to Inventory view in your vSphere client and then you will see the new VM in the list, double-clicking the unconnected NIC, you can turn it on to test See if everything works. When satisfied that it is a successful restore, you can turn off the VM and delete it from the database to free up storage space.

Conclude

Assuming that you have followed the steps guided in this article, then you will have a Data Recovery device to perform backups for you, plus you can test whether it works properly. " *Restore Rehearsal* " feature. One thing to note here is that there are no reporting and warning features, so there is only one way you can check whether your backups are successfully finished. Pay attention to the free space in the backup archive.

It can be said that, although VMware Data Recovery lacks many of the necessary features that are still available in commercial backup applications, it is still a quite useful solution for disaster recovery.

You finished reading the article "**Create and restore backups with VMware vSphere Data Recovery**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.