Some common backup errors

Backup process seems very simple but not so. In fact, many users failed with backup data.

***Network Administration* - For businesses, data is synonymous with money and survival in maintaining business operations. As for computer users, data is also a very valuable thing. Therefore, the need to backup data is becoming increasingly important.**

Backup process seems very simple but not so. In fact, many users failed with backup data. However, it is not due to objective reasons but rather subjective reasons from the users themselves. In this article we will learn some common errors that users encounter when backing up the system.

1. Do not regularly backup the system

In a Windows environment, system state backup files also have an expiration date. With Domain Controller, this time limit is equal to the maximum allowed time (default is 60 days). After that, the backup file will become empty and not valid for use. For other components outside the Domain Controller, the duration of the backup file is also a matter of concern.

Every computer on the Windows network has a corresponding machine account in Active Directory. Like a user account, a computer account also uses a password. The only difference is that the password of the computer account is assigned by Windows operating system and changed periodically. If we try to recover an outdated system state backup file, the password of the computer account stored in this backup file will not match the password assigned to this computer account in Active Directory, Consequently, the computer will not be able to

connect to the domain. Then we can perform some operations to connect this computer back to the domain, but performing the regular server state backup process is much simpler but also helps us protect the data. new material.

2. Do not check backup files

We all know that backup files need to be checked periodically, but this is one of the often forgotten tasks and many administrators have skipped this operation after performing a backup. Remember that backup is only the first operation, as well as a normal data file, for some reason this backup file can also be corrupted, meaning that we will not be able to use it when needed. . Then the consequences will be very unpredictable. Therefore, we need to ensure that every backup file is always in good condition and we can use it when needed.

3. Do not use Application-Aware Backup Application *(backup tool recognizes applications)*

For some applications, file-level backup is not required. A good example of this is Microsoft Exchange software. This software requires users to use an Exchange-Aware Backup Application (Exchange aware backup tool). If you do not use backup tools of this type, all the backed up data will be saved with a conflicting state (and often cannot be restored). Therefore, we need to list every application that is being used on the server and which applications require a separate backup tool.

4. Part of backup data failed

Keep in mind that the backup file system is not just a data protection tool. If a server has a problem, the backup files will be the main tool (sometimes unique) that will make the server work again. Because backup files are especially important, we need to set up an appropriate backup structure to minimize the problem for a certain file in this system. We can backup all backup files. You probably never want to fall into the situation that a backup file made the previous day cannot be used the next day, because then you will have to work in a nervous state of fear of being there is a problem.

5. Not taking into account the consequences of using backup data security solutions

For many companies, IT security is a top priority. However sometimes security is counterproductive. That's when we set the password to protect the backup file, but when we use it, we can't remember the password, or when using a hardware encryption tool, then upgrade to a new hardware device Supporting the previously applied encryption tool, the backup files transferred from the old device cannot be used.

It is undeniable that security of backup data is very important, but we need to consider the consequences of applying security measures to take precautions. If you have to restore a backup file after the system has completely collapsed, then we need to remove the security mechanism that is blocking the recovery process.

6. Only backup data

If you think that you should only back up data to save memory space and time instead of backing up everything in the server operating system and application, it is completely wrong.

In case a server in the network fails and we need to perform a full recovery process, then, if we only back up the data we will have to reinstall the operating system and any of the following applications manually. That restores the data. However, when the incident arises, time is a factor that plays a rather important role because then all activities of the company will be delayed. Then a full backup is really what we need, because restoring

everything from backup data is much faster than manually installing the operating system and applications. More importantly, it is not easy to manually configure a server that matches the previous configuration. Therefore, a full backup for the server not only helps us to conserve data, but also applications and server settings when something goes wrong.

7. Only use a disk-to-disk backup method

Disk-to-disk backup method (using a dedicated backup file server) has many advantages over backup method using traditional storage device. However, we should not use only a disk-to-disk backup tool that needs to use other tools, because the backup server may have the same risks as the servers it does. protect. When a disaster occurs, all systems are affected, so we need to apply traditional backup methods such as using tape, CD, .

8. Storage cycle reuse is too short

Turning around using storage devices is a method that many companies use to save costs. This is a fairly effective method, but it takes a cycle of reusing these devices accordingly. Suppose that when an Exchange server fails in the information storage area, we will have to perform a backup of the backup data, but since the disk reuse time is too short the entire backup drive contains data. error, because this error has existed before and we only know it when something goes wrong. And the result is that the server failed to recover. In this case, in addition to periodically checking backup data, we need to plan to rotate using the storage drive accordingly, it is best to set aside some drives to store the important data. important.