Journal of Computing and Electronic Information Management

ISSN: 2413-1660

Design and Implementation of server data security solutions

Qiuying Han

School of Computer Science and Technology, Zhoukou Normal University, Zhoukou 466001, China;

hanqiuying@zknu.edu.cn

Abstract: The security of server data is the most important in the server management. A set of data security scheme is designed and implemented in the paper: the scheme mainly adopted the techology of data redundancy, data backups are regularly done in the local host and automatically synchronized to the mass storage server. The important server data could be regularly and automatically backuped to the mass storage server without the care of people. Data could be recovered timely through the backups when they are damaged. Thus, the security of server data could be effectively ensured and the possibility of the damage to important data could be effectively reduced at the same time.

Keywords: Linux; server data security; data backup; automatic synchronization

1. Introduction

1.1 Background and significance

As e-government, e-commerce and the development of global informationization, more and more countries functional departments, enterprises and institutions and large enterprise equipped with the server for its own information system construction. Due to the limitation of the server's own hardware technology and the operation level of the technical personnel, the server can not achieve 100% failure. Store huge amounts of data on the server, especially large enterprise server in the event of failure, will directly cause the server to store huge amounts of data is lost, causing national functional departments, enterprises and institutions and serious disaster data of large enterprises. The rising popularity of in the face of the server, the server data security is facing a huge challenge, while the data backup server as the server data security a last line of defense, is particularly important.

1.2 Relevant research and application status

With the rapid development of computer technology, server database plays a very important role in information society. It is widely used in every field, but with it comes the security of data. Loopholes of the operating system is emerge in endlessly, once the last line of defence was breached, even if we have the evidence monitoring and management measures, the server of the important impact of data loss is incalculable. Business system of database is no longer only exists in the high reliability of network, database and multiple applications connected to the network is not reliable, the information business unit of data in the database is the blood of life, to store information is both important and widely; The unauthorised access to the database has raised concerns and created new problems. Security administrators have configured security policies and technologies in succession, but few can resist attacks and protect their databases. In the face of increasing risks, the state has formulated relevant industry regulations. In the face of privacy protection, data protection and the long-term storage and filing of important information, the data protection of the server is in continuous improvement.

The backup strategy is an important method to ensure the security of server data. Currently popular server data backup method, from the system backups to the user, the system and the test of the whole network is a huge, so how to minimize the system cost is very important for backup, introduce more effective backup method is the main research content of this thesis.

1.3 Main research contents

System management focus mainly concentrated in maintenance system normal operation, able to provide normal service, this often involves a problem of data backup, many system administrators don't too concerned about the security of your server, but often is very interested in the backup image technology, but due to the commercial product hardware and software prices are quite high, therefore tend to choose free software. Rsync is the software that satisfies most of the requirements that are not particularly high. It is not very sensitive to data, and it can be used to store backups of large volumes of small files.

We use rsync software to achieve incremental backup of server data, while avoiding the traffic consumption caused by full backup. On the other hand, it can avoid the loss of data when it is damaged, and can quickly realize the reduction of data files and ensure the safety of data. In addition, the cron service enables regular backups of data files, which can reduce the maintenance workload of administrators.

2. Feasibility analysis of Linux server data security scheme

2.1 Importance of backup

A backup is a way to protect data, with multiple backups of data, without fear of the impact of data corruption. Correctly make backups and ensure the effective and available is very important, because the hardware damage, disaster and man-made wrong operation cause data loss is every enterprise need to avoid, is one of the most commonly used method for data backup. The loss of data if the enterprise think is unacceptable, then you must backup the data, and the backup data and need time to recover after a data loss, and the cost of a comprehensive assessment; If the data offline backups still can't meet the needs of business continuity, so companies will need to consider online real-time backup, namely local high availability cluster or beyond the disaster backup solution.

2.2 Determine the backup content

When backing up and restoring the system, Linux is based on the nature of the file. In Windows registry is very related with the system, the configuration and the software installation is not only the files on the system, thus, reducing system need to be able to deal with the features of Windows software. In Linux, the configuration file is based on the text, in addition to direct dealing with hardware, it is has nothing to do with the system to a great extent, is different from how to backup must deal with the operating system installed on your system and complex details of hardware, Linux backups are packaged reconciliation package of files.

A server database is a software system for storing data. Server as the aggregate of information, database system is the core component of computer information system, it is very important for the security, in the face of changing requirements of commercial pressure, more and more enterprises by doing double backup effectively ensure the safety of the server database system. Therefore, we aimed at the Linux server database, through the local backup and synchronization to mass on the server regularly, when damage to the server database and security threats, timely restore the backup data to ensure data security, reduce the loss to a great extent.

2.3 Factors to consider before backing up

There are several factors that must be considered before a system is backed up or restored. Backup is operating on a regular basis to save important documents, file, or the entire system, and for filing is to long-term preservation of important documents, file, or the whole system operation. To make a successful backup, you must first consider all the factors and devise a strategy for doing the backup. Such as:

(1) Portability;

(2) Whether it is automatically backed up;
(3) Perform the backup cycle;
(4) How long do you need to keep the archive backup?
(5) User interface friendliness;
(6) Whether it is necessary to use compression technology, direct copy or encryption;
(7) Backup medium (considering price, performance and storage capacity);
(8) Whether the remote backup or network backup;
(9) Save a file, a subdirectory, or the entire system.

2.4 Linux server data backup recovery strategy

Select the storage backup software, storage backup technology, need to determine the data backup strategy. The backup strategy refers to the content, backup time and backup mode that needs to be backed up. Each unit should make different backup strategies according to its actual situation. Currently, there are three main backup strategies adopted:

(1) Full backup

Every once in a while to a full backup system, so the backup time interval, once the system failure makes the loss of data, can use the previous backup data back to the last backup. The backup data is the most comprehensive, the most complete, and the recovery is fast; But when the amount of data is very large, it takes up a lot of backup disk equipment, and the backup time is long.

(2) Incremental backup

Make a full backup first, and then make a backup every once in a while, but only back up the content that was changed during this time. Once the data is lost, first restore to the previous full backup, and then restore the daily backup by date to the previous day. Therefore, it has a fast backup speed, no redundant backup data, save the tape space, and shorten the backup time; However, the recovery time is long.

(3) Differential backup

First make a full backup every month, and then back up all the data files that have changed since the last full backup. Once the data is lost, a full backup and a differential backup can be used to restore the state of the fault. The difference backup strategy has all the advantages of avoiding the drawbacks of the above two strategies. First of all, it doesn't have to make a full backup of the system every day, so it takes less time to backup and saves the tape space. Second, its disaster recovery is also very convenient.

3. Design and implementation of Linux server data backup scheme

3.1 Pg_dump and pg_restore

Pg_dump is a tool that prints a postgres database to a script file containing query commands. Script files are text format and can be used to rebuild databases, and can even run on other machines or other hardware systems. Pg_dump outputs the query statements needed to rebuild all user-defined types, functions, tables, index aggregations, and operators; In addition, all data is copied in text format, so it can be easily copied back and easily edited by tools.

Pg_restore is a kind of used to restore the pg_dump create any non postgresql database application in plain text output format, it will be sent to regenerate all user-defined types, functions, including data, tables, indexes, gather all the necessary commands and operators.

3.2 Design and implementation of Linux database backup

(1) Install the database postgresql on the server.

sudo apt-get install postgresql

(2) Start

sudo /etc/init.d/postgresql-8.4 start

(3) Set the password

After the installation, we need to change the password for the postgres user, otherwise we can't use the database server. Run the PSQL command as a postgres system user and enter as follows in the terminal:

sudo su postgres -c psql template1

alter user postgres with password ‘net ‘;

(4) Set the postgre user's password.

sudo passwd postgres

Then enter your own password.

(5) Create database

To create the first database, we'll call it mydb:

su postgres

Transfer to postgres user.

createdb mydb

(6) Type the following command to backup:

/usr/bin/pg_dump-h localhost-p 5432-upostgres-F c-b-f /home/net/backup/autobackup mydb

3.3 Recovery of Linux data

chmod 777 /home/net/backup/autobackup
su postgres
dropdb mydb
created db
pg_restore-h localhost-p 5432-U postgres-W–d db-v /home/net/backup/autobackup

4. Design and implementation of timing data synchronization scheme between mirror servers

4.1 Introduction of cron and crontab

System administrator must perform most of the data backup and synchronization task involves some form of system configuration, relatively large when the jurisdiction of the task, the data quantity is more, but as to operate and have a fixed cycle, using automated script has become inevitable.

Linux provides us with powerful tools for automatic backups, which is cron. Cron is a background process, it is a timed execution tool under Linux, can run in the case of without human intervention, once started, will be implemented according to their own configuration files regularly. We can write a shell script file to backup the files, and then let cron periodically start the script file to back up the data.

Cron service can use the crontab command editor, crontab command in Unix and unix-like operating systems, periodic instruction is executed, is used to set the command from the standard input device reads the instructions, and stored in the crontab file, for after read and execute. Usually, the instructions stored in its crontab daemon activated, crontab often run in the background, every minute check whether to have scheduled work need to be performed, crontab file contains a series of assignments and instructions to the cron daemon. Each user can have their own crontab file, at the same time, the operating system to save one for the whole system crontab file, the file is usually stored in/etc or under the/etc subdirectory, and this file can only be modified by the system administrator.

4.2 Introduction of rsync

Rsync is a fast incremental file transfer tool that can be used to backup internal backups on the same host, and we can use it as a backup tool for different hosts. For tar and wget, rsync has its own advantages, such as fast, safe and efficient. Rsync is a bandwidth saving backup solution, unlike traditional FTP that downloads all files, regardless of whether they are updated or not, and rsync downloads only those updates.

4.3 Design and implementation of Linux server database synchronization

The design and implementation of synchronization of server database is shown in figure 1:

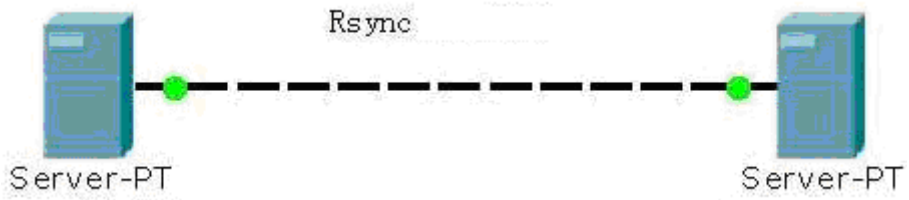

Figure 1. Example of server data synchronization

Installation and configuration of server

(1) Installation of rsync and SSH

sudo–i

apt–get install rsync

apt–get install openssh-server

(2) The configuration of rsyncd. Conf

cp/usr/share/doc/rsync/examples/rsyncd.conf/etc

gedit /etc/rsyncd.conf

Set the path in rsync.conf (the directory that needs to be backed up)

path=/home/net/backup

(3) Create a new file, rsyncd. Pass.

gedit /etc/rsyncd.pass

Content is backup:backup

(4) Modify the permissions of rsyncd. Pass.

chmod 700 /etc/rsyncd.pass

(5) Start rsync

rsync –daemon

(6) After startup, you can use lsof - I :873 to start normally, or check /var/log/rsyncd related log files.

Backup client installation and configuration.

(1) Installation of the rsync

sudo –i

apt–get install rsync

(2) The setting of crontab

gedit /etc/crontab

Content : */1 * * * * root /home/net/test.sh

sudo gedit /home/net/test.sh

Content : rsync -vzrtopg --progress --delete backup@192.168.230.128:: rsync/home/net/backup --password-file=/etc/rsyncd.pwd

sudo chmod 700 /home/net/test.sh

ls–l /home/net/test.sh
gedit /etc/rsyncd.pwd
Content : backup
chmod 700 /etc/rsyncd.pwd

5. Conclusion

Linux is a stable and reliable environment, but any computing system has unpredictable events, such as hardware failures. A reliable backup with key configuration information is part of any responsible management plan. In Linux, you can perform backups in a variety of ways, from very simple script-driven approaches to well-designed commercial software; Backups can be saved to remote network devices, tape drives, and other removable media; Backups can be file-based or drive-based, with many options available, mixed with these techniques, and can design an ideal backup plan.

In this thesis, the security of data can be effectively guaranteed by backing up data to local and remote synchronization to another massive server. In this design scheme, on the one hand, using cron and rsync technology to realize regular backup and synchronization of data can effectively guarantee the security of the server data at all times; Using pg_dump and pg_restore, on the other hand, can make the data leads out again after compression backup and synchronization, can reduce the backup and synchronization caused by traffic, in guaranteeing data security and ensure the normal operation of the server.

References

[1] Wang sheng, wang yi. Overview of Linux real-time file backup system [J]. Computer and modernization,2009,(6):40-43.
[2] Yu lingzhi. Remote synchronization of Linux platform data [J]. Webmaster world, 2006, (11):100-102.
[3] Jiang hong. Make a backup copy of Linux [J]. Open system world.2004,(5):50-51.
[4] Wu jingwen. Research on Linux backup strategy [J]. Webmaster world. 2005, (8): 26-27.
[5] TuJunYing. Linux system data backup strategy research [J]. Journal of electronic commerce in China, 2010, (9) : 59-59.
[6] Dong Xiulei. Implementation method of data automatic backup in Linux system [J]. China education,2009,(10):27-28.
[7] Sun hao. Setting up backup for Linux system [J]. Open system world,2006, (1): 77-78.
[8] Wang fei fei. Linux backup and repair technology [J]. Open system world, 2007, (3):38-40.
[9] Wang moon. A brief discussion on data backup in Linux [J]. Open system world, 2008, (1):76-78.