Disaster Recovery Plan: Automating Backup Process for Library Databases

Vijaykumar Shrimali *Nabila Shaikh*

Abstract

Information Technology (IT) has intertwined with our day-to-day lifestyle in communication, professionalism of the business and meetings, learning and teaching, tourism and even entertainment are connected by the IT Tools. Normally, we do not realize these roots of IT. But if suddenly any service is stopped because of any disaster then importance is realized at organizational as well as personal level. Organization must ensure the recovery of each and every IT related tools to make them always functional. In this article, efforts are made to automate backup as part of Disaster Recovery Plan which will be useful to library in case of disaster.

Keywords: Disaster Recovery Plan, IT Disaster, Database Backup, SQL Server, SOUL 2.0, Auto Backup

1. Introduction

"A Disaster is a serious disruption of the functioning of community or a society involving widespread human, material, economic or environmental losses and impacts which exceeds the ability of the affected community or society of cope using its own resources." is a definition by Wikipedia.

Disaster may damage any type of infrastructure and lives. At present most organizations are fully or partially dependent on Information Technology infrastructure which can also be affected if disaster occurs. To put the definition in our term, IT Disaster means unplanned interruptions of any routine business processes by the failure of Information Technology infrastructure of organization.

2. Causes of IT Disaster

IT disaster may be caused by failure of any IT related component i.e. application software, utility software, hardware tools, networking applications or hardware, data tools etc. Most disasters could happen by man-made mistakes. Some of are accidental and others intentional. Aside from any manmade mistakes, natural calamities also endangers IT infrastructure which is most critical and incapable of 100% recovery.

2.1. Types of Disaster

2.1.1. Man-Made

2.1.1.1. Accidental

2.1.1.1.1. Operating system failure by virus, malware

2.1.1.1.2. Overwriting of operating system or data files

2.1.1.1.3. Deletion backup files or operational data by mistake

2.1.1.1.4. Hardware damaged physically or functionally

2.1.1.1.5. Networking cables or devices being damaged

2.1.1.2. Intentional

2.1.1.2.1. Terrorist activities

2.1.1.2.2. Formating of hard disk without precaution of backup

2.1.2. Natural

2.1.2.1. Fire, flood, earth quake, shot circuit in server room/data center etc.

3. Rescue Plan for IT Disaster

There must exists Disaster Recovery Plan (DRP) for organization. DRP is documented process of objectives and action plan at organization level. It includes all information regarding data backup strategy, licensed software, hardware details, alternate or mirror server details with credential, vendor details for reorder or maintenance, contact details of all project heads etc. Besides it also has alternative disaster recovery team which comes in action after any disruptive event. DRP plan's offline copy should be available with all responsible persons of the organization. If allowed, online copy can also be shared with privileged users. Most organizations tends to neglect disasters and their plan for recovery. It is also true that there is no 100% recovery plan because no one can assume future. Still only option is available to find out possibilities of failure and prepare recovery plan.

In IT Disaster recovery plan, Hardware part will be repaired or replaced with new instruments. Software must be reinstalled in new setup. But data part is most crucial to recover in different scenario.

In context of library, every institute is either fully or partially automated for routine library task and innovative services. Automation itself depends on IT Infrastructure like server, automation software, supporting application utilities, barcode scanner, printer etc. Most important thing is data which includes details of procurement, bibliographic, membership, circulation, authority files etc. They are saved in one centralized database so that it is available to continue library's routine task.

4. Background

As members of SOUL Support Cell, it may observed that most libraries lose their data in manmade disasters. They may not be aware of backup process or not that much keen to understand importance of backup. Many libraries then restored old backup and continue from earlier point in time. Some cases are, failure of hard disk, using a decade old systems, not taking routine backup, deleting files unknowingly. Visit to flood affected colleges of Srinagar, Kashmir where most premises were have lost their entire institute infrastructure including databases comes in this context. To overcome this type of situations, database backup must be kept in different locations.

5. Objectives

As a part of DRP (Disaster Recovery Plan), the objective is to create automated backup plan to rescue the information from any disaster. For this one can create a batch (.bat) which is normally used to automate windows task without using any third party tool. As mentioned above disasters in some cases, may affect single machine only and in some

cases can affect whole or partial IT infrastructure itself. In natural disaster, much bigger geographical area can be affected instead of a building. So in traditional practice professional DBAs store backup in multiple locations in different media to overcome from this type of issues. Considering each case, some automated options need to be identified that can store the database backup on different locations.

It involves below tasks,

- ❖ Identification type of backup will be useful in case of failure.
- ❖ Create Scripts to backup on different locations.
- ❖ Compose scripts in one file and scheduled as daily task.

6. Case Study

The case considered here in this article is the ILMS (Integrated Library Management Software) SOUL 2.0 installed at server system of the library with below system configurations:

- ❖ Database software (Microsoft SQL Server 2005)
- ❖ Operating System (Windows)
- ❖ Networking with internal machines & internet connection

6.1. What is Backup?

Database backup is the process to save information of database operation state, architecture and all processed data.

6.2. Backup Types

There are different types of backup options available through Microsoft's SQL (Full Backup, Differential Backup, Transaction Log Backup, SQL Server File backup etc.) By default the SQL is bound to take full backup that includes all database files. In case the full backup file of database is large then one should consider differential backup for rescue plan. Full backup option also includes transaction log which makes it easy to restore. On the other hand, Differential Backup is a backup of data that has changed after last full backup. In this case, Full backup is considered for Disaster Recovery Plan.

6.3. Backup Process

6.3.1. Backup on Local drive

Local drives are the partition of disk space that is available in every computer machines. One drive out of all the partition is called the root drive with system files of operating system and software indexing files etc. Taking backup on a local drive is a routine task and it should be scheduled with the human operations. Database backup is stored on the local drive and also it should be done every day without fail.

6.3.1.1. Script

The following backup procedure is adapted through Microsoft's SQL Query Execution by using SQLCMD, command line tool

```
SQLCMD -U username -P password -S server -Q
"BACKUP DATABASE dbname to DISK =
"D:\SOULbkp\soul20.bak" WITH PASSWORD =
password, STATS, DESCRIPTION = 'Full backup
of SOUL 20 Database'"
```

Parameters and additional arguments

U = Mention the SQL Server User Name (By default 'sa').

P = Mention SQL Server password for the mentioned user.

S = Server Name.

Q =SQL Query.

DBNAME = Database Name.

BACKUP PATH = Complete Address of the main folder starting from the drive (For ex: D:\SOUL\).

WITH PASSWORD = Must provide the same password at the time of backup restore.

WITH STATS = Shows progress of backup task (by default 10%).

DESCRIPTION = Description of backup file (maximum 255 chars).

WITH COMPRESSION = To reduce backup size in order to save disk space (option available only with SQL 2008 or later versions).

Command must be saved in batch file having .bat extension which can be executed as a windows command line file.

6.3.1.2. Restore Scenario

This backup will be restored in mentioned disaster caused, failure of software instance, database server instance, etc.

6.3.1.3. Note to Self

Backup should never be stored on the root drive or recovery drive which comes in the latest version of Windows Operating Systems (generally drive C:) instead the backup folder must always be created in other drive which may be safe from the operating system crash.

6.3.2. Network Drive

Creating a backup on local drive is an offline option to be used only when the institute infrastructure is limited or is affected by the cost factor. IT can offer various options which can be explored if human resources with the knowledge of advance system are available. Taking backup on network drive is one step ahead than a local drive backup. A network drive is partition of disk space that is available not locally on your machine but on more safe system for example server system that cannot be easily accessed by viruses or malwares or by normal users. This option is usable when the current system's failure is a greater possibility. The path of a network drive is accessed by using computer name or computer's IP address. Same command is used to save backup to network drive.

6.3.2.1. Script

```
SQLCMD -U username -P password -S server -Q
"BACKUP DATABASE dbname to DISK =
"\\VIJAY\SharedInNetwork\soul20.bak" WITH
PASSWORD = password, STATS, DESCRIPTION
= 'Full backup of SOUL 20 Database in Network
Drive'"
```

6.3.2.2. Restore Scenario

This backup file will be used in below disaster caused. i.e. operating system failure, hard disk failure, database backup file deleted or overwritten by old file, theft of hard disk/system,etc.

6.3.2.3. Note to Self

Access to the networked drive and folders must be allowed to the authorized user who is in charge of taking backup.

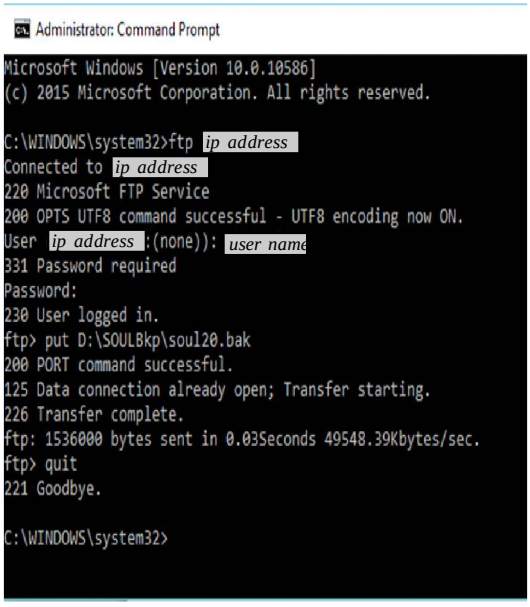
6.3.3. FTP Server

FTP site server is an advance option compared to network drive as availability of FTP site range is wider than the network drive. FTP site server should be available outside campus in other network range, far away from the user's machine. Normally SQL server does not allow direct FTP drive path for backup so it must be mapped with network drive. Alternatively backup can be saved in local temporarily and then copy can be sent to FTP server. Same idea is implemented in below given script.

FTP server credential must be known to the user in-charge to work with FTP server.

6.3.3.1. Script

```
FTP ftpservername (will ask for FTP server ID/ Password for connection)
Put D:\SOULBkp\soul20.bak
Quit
```



In order to run the commands through batch file, the same command-line process has to be converted in the following code:

```
@echo off
echo user username >ftpcmd
echo password >>ftpcmd
echo bin>>ftpcmd
echo put D:\SOULbkp\soul20.bak >>ftpcmd
echo quit >>ftpcmd
ftp -n -s:ftpcmd servername
```

6.3.3.2. Restore Scenario

It will be used to restore when broad geographic area may be affected in major disaster.

6.3.3.3. Note to Self

North East region generally faces flood and earth quake. In broader way choose FTP site as per disaster zone. For example user can refer climate disaster map, earth quake zone map etc. on website http://www.mapsofindia.com/. One can identify safe zone for database backup in any major disaster.

6.3.4. Email

Taking backup through email is an option that is freely and openly available to all the users of IT and the requirement of infrastructure are less and server costing is not important. Copying the backup file or directly taking backup and emailing it on email server is the option that might be bit technical but yet very secure in terms of safety. The case taken, as example in the email option, is for Google's email facility – known as Gmail.

To send email without using any third party tool even Google's Gmail interface, used powershell script. It is command line utility which is used for

dotnetframework programming. It is in built in all windows later than Windows XP.

6.3.4.1. Script

```
$EmailTo = "recipient's email ID"
$EmailFrom = "sender's email ID"
$Subject = "Email Subject Heading"
$Body = "Email Body Text"
$SMTPServer = "smtp.gmail.com"
$filenameAndPath = "The Local Drive Path/Address"
$SMTPMessage = New-Object
System.Net.Mail.MailMessage($EmailFrom,$EmailTo,$Subject,$Body)
$attachment = New-Object System.Net.Mail.Attachment($filenameAndPath)
$SMTPMessage.Attachments.Add($attachment)
$SMTPClient = New-Object Net.Mail.SmtpClient($SmtpServer, 587)
$SMTPClient.EnableSsl = $true
$SMTPClient.Credentials = New-Object System.Net.NetworkCredential("sender's email ID",
"password");
$SMTPClient.Send($SMTPMessage)
```

6.3.4.2. Restore Scenario

It will be evergreen & most trusted option but only internet connection is a must for download.

6.3.4.3. Note to shelf

If backup file is greater than 25 MB then in cannot be attached in email. In that case, choose differential backup followed by initial full backup. In SQL server later than 2008, WITH COMPRESS option is also there in BACKUP command, for compressed backup file.

Gmail is secured and does not allow by default to send email by using it's credential. Turn on ALLOW LESS SECURE APPS option to send email via Gmail credential without using Gmail interface.

One can use any other SMTP service instead of Google to implement this task like Yahoo, Rediff, etc.

7. Consolidate All Processes in ONE file

Idea is to schedule this task automatically by using the windows task scheduler. In that case backup file cannot be saved with same name otherwise process will overwrite last backup every time. Finally backup file size will be increase on that level which may not be easily manageable.

User can add the backup file name with %DATE % parameters to keep it in different name every time instead of overwriting the same file.

i.e. 'D:\SOULbkp\%Date%_soul20.bak'

Another facility is there in command prompt to save command output. User can create text file & include at the end of every main command in this batch file. By using this, log file can be managed.

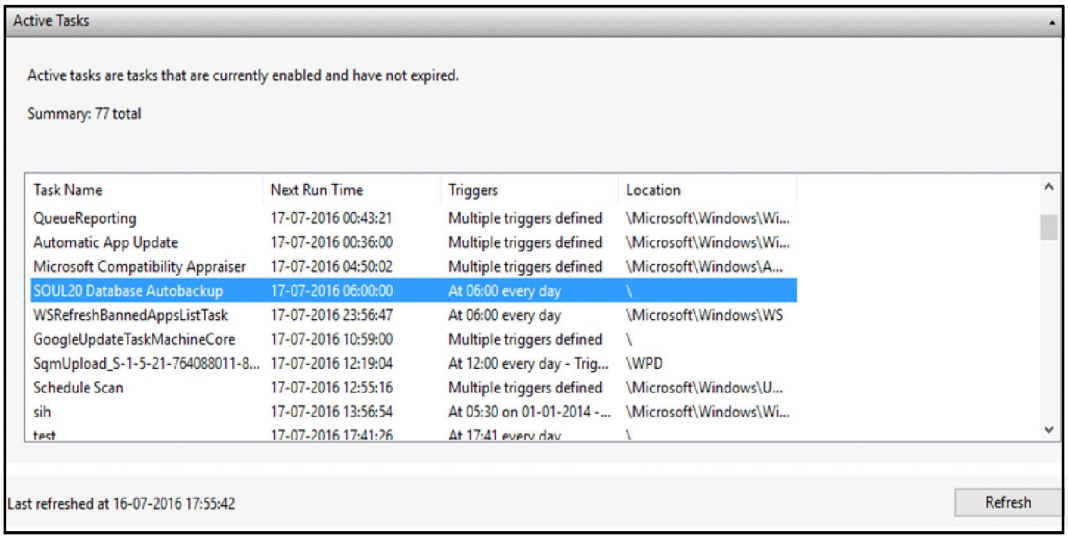
COMMAND >> D:\SOULBkp\autobkp.txt

All scripts can be easily saved in one batch file and looks like asdisplayed below.

```
SQLCMD -U sa -P password -S servername -Q "BACKUP DATABASE soul20 to DISK ='D:\SOULbkp\%Date%_soul20.bak'
WITH STATS, DESCRIPTION ='Full backup of SOUL 20 Database taken on %Date%'">>D:\SOULBkp\autobkp.txt

SQLCMD -U sa -P password -S servername -Q "BACKUP DATABASE soul20 to DISK = '\\VIJAY\SharedInNetwork\%Date%_soul20.bak'
WITH STATS, DESCRIPTION ='Full backup of SOUL 20 Database on Network Drive taken on %Date%'" >> D:\SOULBkp\autobkp.txt

@echo off
echo user ftpusername>ftpcmd
echo ftppassword>>ftpcmd
echo bin>>ftpcmd
echo put D:\SOULbkp\%Date%_soul20.bak>>ftpcmd
echo quit>>ftpcmd
ftp -n -s:ftpcmd serverip >> D:\SOULBkp\autobkp.txt

@echo off
echo $EmailTo = "xyz@gmail.com">email.ps1
echo $EmailFrom = "abc@gmail.com">>email.ps1
echo $Subject = "SOUL 20 AutBACKUP">>email.ps1
echo $Body = "Dear Sir/Madam, Please find herewith attached backup of SOUL20 database generating on %TIME%
%Date%.">>email.ps1
echo $SMTPServer = "smtp.gmail.com">>email.ps1
echo $filenameAndPath = "D:\SOULbkp\%Date%_soul20.bak">>email.ps1
echo $SMTPMessage = New-Object System.Net.Mail.MailMessage($EmailFrom,$EmailTo,$Subject,$Body)>>email.ps1
echo $attachment = New-Object System.Net.Mail.Attachment($filenameAndPath)>>email.ps1
echo $SMTPMessage.Attachments.Add($attachment)>>email.ps1
echo $SMTPClient = New-Object Net.Mail.SmtpClient($SmtpServer, 587)>>email.ps1
echo $SMTPClient.EnableSsl = $true>>email.ps1
echo $SMTPClient.Credentials = New-Object System.Net.NetworkCredential("abc@gmail.com", "password");>>email.ps1
echo $SMTPClient.Send($SMTPMessage)>>email.ps1

powershell -executionPolicy bypass -file email.ps1
```

8. Testing

It must pass through testing as required at the end of any software creation. Execute that file and check in all locations to check database backup is saved or not.



9. Schedule task for automatic backup

Windows has task scheduler tool which is used to automate or schedule any task. User can create Schedule for creating script to automatic backup task.

10. Conclusion

Here SOUL 2.0 ILMS is chosen as an example since many institutes are using SOUL 2.0 for library automation in North East Region. Some areas of North-East are very well developed in terms of IT whereas many areas are yet to have such facilities. The backup types are considered by keeping in mind all libraries which use computers. It is just an example of SOUL database backup, but user can take backup of any database and important files, send email alerts or perform any administrative task to minimize the downtime of library services in any type of failure.

References

1. MICROSOFT, Planning for Disaster Recovery, https://technet.microsoft.com/en-us/library/ms178094(v=sql.105).aspx
2. MICROSOFT, Data Backup and Recovery / Chapter 14, https://msdn.microsoft.com/en-us/library/bb727106.aspx
3. MICROSOFT, Schedule a Task, https://technet.microsoft.com/en-us/library/cc748993(v=ws.11).aspx
4. Wikipedia, Disaster recovery plan, https://en.wikipedia.org/wiki/Disaster_recovery_plan
5. TechRepublic, Send an email with an attachment using PowerShell, By Harold Ogden | in

Windows and Office, August 31, 2011, 5:30 AM PST, http://www.techrepublic.com/blog/windows-and-office/send-an-email-with-an-attachment-using-powershell/

About Authors

Mr. Vijaykumar Shrimali , STA-I(CS), INFLIBNET Centre, Gandhinagar, Gujarat
Email: shrimali@inflibnet.ac.in

Ms. Nabila Shaikh, Project Officer (CS), INFLIBNET Centre, Gandhinagar, Gujarat
Email: nabila@inflibnet.ac.in