International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

Survey Paper : Backup and Restore Techniques in Exchange

Manushree N[1], Dr. K.V Nagalakshmi[2]

[1]*NIE, Mysuru, Karnataka, India*
[2]*Asst. Professor, Dept. of ECE, NIE, Mysuru, Karnataka, India*

Abstract - *In day-to-day IT operations, backup and disaster recovery play a vital role. They describe several aspects of a company's business continuity plan. Because organizations' valuable and vital data is housed in a data domain or a remote place on the cloud, we must ensure that user data is safe and accessible at any times. Our data may become unavailable in the event of a flood, fire, earthquake, or any hardware fault or inadvertent deletion. There must be some data backup solution for data domain or cloud platform to restore valuable and vital data rapidly to maintain data security and availability. We conducted a survey of different backup and restore mechanisms utilized in Exchange server in this research.*

Key Words: **Exchange Backup, Exchange Restore, Disaster Recovery, DAG, RPO, RTO, Database, Mailbox.**

1. INTRODUCTION

As data is at the heart of the enterprise, it becomes both critical and important for us to protect it. We also need to implement a data backup and recovery plan to protect our organization's data. File backups can protect against data loss due to human error, database corruption, hardware problems, and even natural disasters. .As an administrator, it is our responsibility to ensure that backups are performed and stored in a secure location. A backup, or the process of backing up, in information technology refers to the copying and archiving of computer data in order to restore the original following a data loss incident.

There are two distinct objectives for backups. The main goal is to recover data that has been lost due to deletion or corruption. The secondary purpose of backups is to restore data from an earlier point in time, based on a user-defined data retention policy, which is often set up within a backup application and specifies how long copies of data must be retained[1].

Though backups are commonly thought of as a simple type of disaster recovery and should be included in any disaster recovery plan, they should not be considered disaster recovery in and of itself. One reason for this is because not all backup systems or backup apps can simply restore data from a backup to recreate a computer system or other sophisticated configurations like a computer cluster, active directory servers, or database servers.

The data storage needs of a backup system might be significant because it contains at least one copy of all data worth saving. Managing the backup process and organizing this storage space might be a difficult task. To provide structure to the storage, a data repository model might be used.

With the advancement of technology, there is a greater demand for reliable, low-cost, and low-burden techniques for businesses to restore lost data from backup copies. With the expansion of apps and the existence of many devices, there is a demand for backup and disaster recovery plans that have greater data integrity, the capacity to handle a large number of devices at once, and the ability to recover data efficiently[2]. Due to the cost of recreating lost data, dilatory, legal actions that may be faced, and lower productivity, the absence of a backup operation scheduled to take place in an enterprise may have a significant financial impact on the enterprise, eventually leading to the business's collapse. [3].

2. Backup and restore for Exchange

Database Availability Groups (DAGs) in Exchange Server serve to keep stored data secure and available while reducing the requirement for specialized backup and restore applications. DAGs enable for off-site data redundancy, ensuring that data is never lost. Many disaster recovery plans continue to employ more traditional backup and restore methods and technologies, including custom applications, for redundancy with the DAG. That helps assure data availability and redundancy in an organisation by backing up and restoring Exchange data using Exchange Server and Windows Server operating system technologies

Administrators can use a plug-in for Windows Server Backup in Exchange 2010-19 to make VSS-based backups of Exchange data. Windows Server Backup can also be used to back up and recover Exchange databases.

2.1 VSS Writer in Exchange

VSS organizes the actions necessary to make a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data being backed up. The shadow copy can be used as-is, or it can be used in scenarios such as the following[4]:

- Want to archive data to another hard disc drive, tape, or other removable media, as well as back up application data and system state information.
- Performing disk-to-disk backups.
- Data mining.
- Data loss can be quickly recovered by restoring data to the original Logical Unit Number (LUN) or to a totally new LUN that replaces a failed original LUN.

Exchange include two VSS writers:

one in the Exchange Information Store (store.exe) and the other in the Exchange Replication service (msexchangerepl.exe).

In Exchange 2013 and later versions, the VSS writer functionality is located in the Exchange Replication service. Backup and restore application use the new VSS writer, called the Microsoft Exchange Writer, to back up active and passive database copies, and to restore backed up database copies. Although the new VSS writer runs in the Exchange Replication service, the Exchange Information Store service must be running in order for the writer to be available. As a result, both services are required to back up or restore Exchange databases.

2.2 Exchange Store Database files

Exchange support for up to 100 databases. Each Exchange database contains the files listed below[5]:

Database file (.edb) : Records all the changes that have been committed to the in-memory database.

Transaction log stream (.log) : Records operations, such as the creation or modification of a message, that will be committed to the database. Limited in size to 1 MB each.

Checkpoint file (.chk) : Records which logged transactions have been written to the on-disk database files.

For each database, Exchange keeps a single set of transaction log files. Backup and recovery processes rely heavily on transaction logs. When you utilize the Volume Shadow Copy Service to develop a backup and restore application (VSS).

3. Types of backup and restore in Exchange

3.1 Backup types

Full backups : Backs up the databases (*.edb), transaction logs (*.log), and checkpoint files (*.chk) for a specific database, and then truncates the transaction logs.

Copy backups : The database, transaction logs, and checkpoint files are all backed up. The transaction logs for the database are not truncated by copy backups.

Incremental backup : The transaction logs are backed up to capture changes since the last complete or incremental backup, and then truncated.

Differential Backup : The transaction logs are backed up to capture changes since the last complete or incremental backup, and they are not truncated.

Synthetic full backup : It's a backup that combines the most recent full backup with subsequent incremental or differential backups to build a synthesized backup.

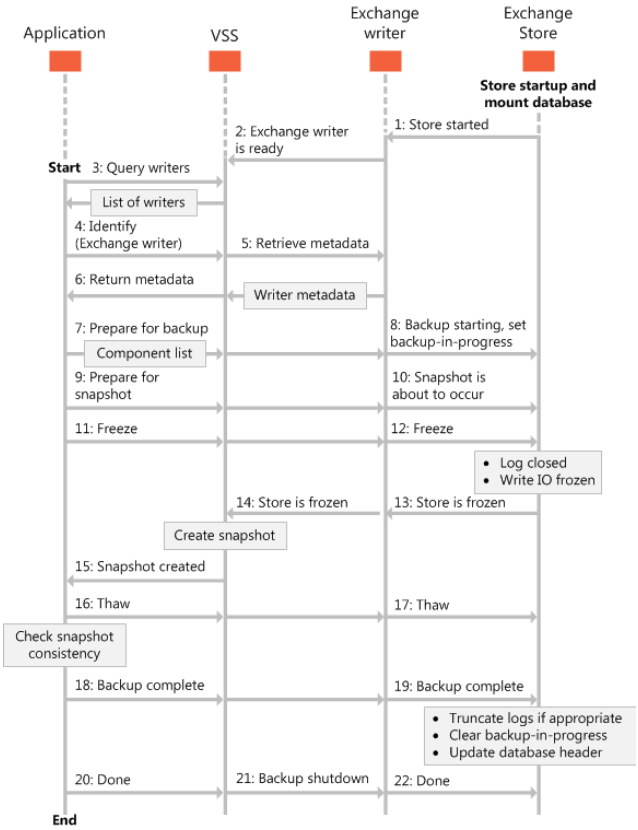

Fig-1: Sequence of events for backup process

The database files and transaction logs within Exchange databases are represented by the components, or database files, defined by the Exchange writer. During backup operations, your backup and restore application can display the names of the components in an Exchange database. backup application cannot back up individual database components, however; it can only back up whole databases[6].

The fig 1 shows the sequence of events in a backup process of an Exchange database that is managed by the Volume Shadow Copy Service (VSS). Based on the VSS

framework guidelines, the Exchange writer only lists databases that can be backed up. Databases that are mounted as the Exchange recovery database, as well as databases that are not mounted, cannot be backed up and are thus not listed in the metadata of the Exchange writer.

3.2 Restore Types :

The various types of restore are listed below [11] :

Roll-forward - When databases in the storage group are lost but the transaction log files are still intact, this recovery procedure is employed.

Point-in-time - When only transaction log files or both transaction log files and database files are lost, this recovery procedure is employed.

Full restore - When the entire storage group (databases and log files) must be restored from a full backup, this recovery method is used.

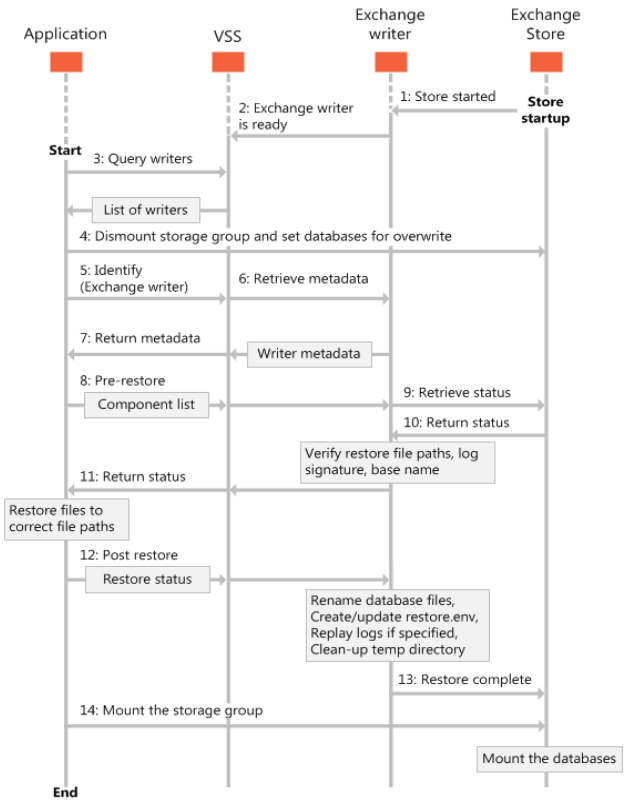

Fig-2: Sequence of events for restoring databases

The log files must be restored to the directory path defined in Active Directory Domain Services (AD DS) for that database when your restore application restores information to the original database. If your application restores a database to a new location, the log files must be restored to the _restoredLogs folder within the database log file directory.

Restore application must ensure that the database directory paths provided to VSS match those in AD DS when restoring to a different server or database than the original database. You can use the get-MailboxDatabase Exchange Management Shell cmdlet.

Fig 2 depicts the events involved in restoring an Exchange database via the Volume Shadow Copy Service (VSS)[7].

3. Disaster Recovery

A disaster is an unexpected incident that occurs within the lifespan of a system. It can be caused by the environment (such as a tsunami or an earthquake), as well as hardware or software faults. Because of its ability to accept disasters and provide consistency and availability, cloud-based DR solutions are becoming more popular.

3.1 success metrics for disaster recovery :

You must first identify the success metrics for the exercise before planning the recovery paths and techniques to restore critical Exchange services. This stage will assist you in achieving the end goal within the required time frame (SLA) and database state as determined by your organization's standards[8]:

A) Recovery Point Objective (RPO):

This is the “point in time” before the disaster event to which the server state and operations can be restored in case of a failure event. For example, if you take a daily full back up at 1:00 AM and the failure happens at 5:00 a.m., the RPO is 1:00 a.m. Therefore, to be successful, you should be able to restore the Exchange database and other critical services to their particular state at 1:00 AM. The RPO establishes the maximum amount of data your organization can afford to lose in case of a disaster. So, it provides essential input for defining the “backup frequency and schedule.” This would also involve other mechanisms like high availability to counter data loss or reduce the data loss period.

B) Recovery Time Objective (RTO):

After a disaster, this is the "maximum time allowed" to restore Exchange services and mailbox databases. RTO is an important part of the SLA for restoring the system and gives essential information for defining backup and restore operations. The RTO, which is measured in seconds, minutes, days, and other units, is important for disaster recovery planning in Exchange. RTO also aids in calculating the “backup size” that should be considered when comparing to the SLA. For example, if backing up and restoring 300GB of

data takes around 1.5 hours and the SLA is six hours. The size of your backup should be less than 1.2TB.

3.2 Choose the Exchange backup strategy :

This step is all about deciding which backup type to use for an on-premises Exchange Server. The purpose is to save one or more point-in-time copies of the on-premises Exchange mailbox database and services so that they may be restored in case of a failure event.

The RPO and RTO provide essential information for selecting a backup strategy. The "time to restore" is almost twice as long as the "time to back up," because the restore time includes the time it takes to identify the failure event, try to debug the problem, locate and initialize the backup media, restore the backup, and replay the transaction logs.

3.3 Scenarios where backup have been used :

Traditionally, backups have been used for the following scenarios[9]:

Disaster recovery: In the event of a hardware or software failure, multiple database copies in a DAG enable high availability with fast failover and little or no data loss. This eliminates the downtime and lost productivity that comes with recovering from a previous point-in-time backup to disc or tape. DAGs can be extended to numerous sites and offer disaster recovery in the event of disc, server, network, or datacenter failures.

Recovery of accidentally deleted items: In the history, if a user deleted items that later needed to be retrieved, the process entailed first locating the backup media on which the data needed to be recovered was saved, and then locating and delivering the requested objects to the user. It's possible to retain all deleted and modified data for a predetermined length of time with the Recoverable Items folder in Exchange 2016 and Exchange 2019, as well as the Hold Policy that may be applied to it, making recovery of these items easier and faster. By allowing end users to recover accidentally deleted items themselves, Exchange administrators and the IT help desk are relieved of the complexity and administrative costs involved with single item recovery.

Long-term data storage: Backups have also been used as archives, and tape is generally used to store point-in-time copies of data over long periods of time as required by compliance regulations. Exchange Server's new archiving, multiple-mailbox search, and message retention features give a way to efficiently retain data in an end-user accessible format for long periods of time. This eliminates expensive restores from tape and increases productivity.

Point-in-time database snapshot: If a past point-in-time copy of mailbox data is a requirement for your organization, Exchange provides the ability to create a lagged database copy in a DAG environment. This can be useful if a store logical corruption spreads over many database copies in the DAG, necessitating a rollback to a previous point in time. It may also be useful if an administrator accidentally deletes mailboxes or user data. Because delayed copies don't require a time-consuming copy process from the backup server to the Exchange server, recovering from a lagged copy can be faster than recovering from a backup. By limiting downtime, this can drastically cut total cost of ownership.

4. CONCLUSIONS

In this survey paper, We discussed Exchange backup and restore, Exchange disaster recovery, and a few key points, such as the importance of testing the recovery plan and the complexity of the database backup aspect in the planning; backing up the database includes a variety of options, such as the type of backups, backup destination, frequency, Importance of VSS writer and it's types and types of restore and so on. Regarding the scenarios that arise as a result of log file truncation and circular logging as a result, thorough examination of the mailbox database backup technique is critical to the overall disaster recovery plan's effectiveness. In addition, third-party software should be included in the overall Exchange Server disaster recovery strategy to enable for seamless mailbox recovery in the event of unanticipated events such as database or backup file corruption, which can occur for a numerous reason.

REFERENCES

[1] Zaman, M., 2013. Enterprise Data Backup & Recovery: A Generic Approach. IOSR Journal of Engineering, 03(05), pp.40-42.

[2] O. P. Rotaru, "Beyond Traditional Disaster Recovery Goals–Augmenting the Recovery Consistency Characteristics," in Proceedings of the International Conference on Software Engineering Research and Practice (SERP), 2012, p. 1.

[3] "Disaster Recovery: Best Practices [High Availability]," Cisco. [Online]. Available: <http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11- 453495.html>.

[4] Docs.microsoft.com. 2021. Volume Shadow Copy Service. [online] Available at: <https://docs.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service>.

[5] Docs.microsoft.com. 2021. Backup and restore concepts for Exchange 2013. [online] Available at: <https://docs.microsoft.com/en-us/exchange/client-developer/backup-restore/backup-and-restore-concepts-for-exchange-2013>.

[6] Docs.microsoft.com. 2021. Types of backup operations for Exchange 2013. [online] Available at: <https://docs.microsoft.com/en-us/exchange/client-

developer/backup-restore/types-of-backup-operations-for-exchange-2013>.

[7] Docs.microsoft.com. 2021. Restoring Exchange 2013 databases. [online] Available at: <https://docs.microsoft.com/en-us/exchange/client-developer/backup-restore/restoring-exchange-2013-databases>.

[8] TechGenix. 2021. Exchange Server disaster recovery: Step-by-step planning. [online] Available at: <https://techgenix.com/exchange-server-disaster-recovery/>.

[9] Docs.microsoft.com. 2021. Exchange Server data protection, Exchange disaster recovery, Exchange backup, Exchange VSS Writer, VSS Backup Exchange, Exchange Server data recovery, Exchange data recovery. [online] Available at: <https://docs.microsoft.com/en-us/exchange/high-availability/disaster-recovery/disaster-recovery?view=exchserver-2019> [Accessed 26 July 2021].

[10] A. Chervenak, V. Vellanki, and Z. Kurmas, Protecting File Systems: ASurvey of Backup Techniques. proceedings Joint NASA and IEEE Massstorage,1998.

[11] Support.carbonite.com. 2021. Carbonite Support Knowledge Base. [online] Available at: <https://support.carbonite.com/articles/Server-Windows-Restoring-a-Microsoft-Exchange-Server>.