MODULE - III

Backup and Recovery

MODULE 3

Backup and Recovery

Module Description

Data, today, has become an essential entity for enterprises. Ensuring the storage, management and protection of data has become a necessity for the organisations. In the previous modules, we have read about the storage and management of data. This module caters to the protection, backup and recovery of data.

To protect the data, it is a smart choice to create its backup and to have processes in place that can recover the lost data. Backup and recovery refers to several procedure and strategies that are required for protecting the database against any kind of data loss and reconstructing the database post data loss.

In this module, students will get an insight on the purpose of backup and recovery, backup methods and processes and backup technologies. Students will also get to know about backup topologies, backup granularity and recovery considerations.

Chapter Table of Contents

Chapter 3.1

Introduction to Backup and Recovery

Aim

To equip students with the fundamentals of backup and recovery

Instructional Objectives

After completing this chapter, you should be able to:

- Explain the purpose of backup in the system
- Elaborate the concept of disaster recovery
- Explain the concept of the operational backup
- Explain the considerations to create backup
- Describe the concept of backup granularity and recovery considerations
- Discuss the various backup methods and backup processes
- Explain backup and restore operations

Learning Outcomes

At the end of this chapter, you are expected to:

- Identify the purpose of backup and disaster recovery
- Outline the operational backup and data archival
- Identify the important considerations to create backup
- Discuss the backup granularity
- Outline the considerations to recover data
- Identify the effective backup methods and processes
- Outline backup and restore operations

3.1.1 Introduction

“Marco Marsala accidently deletes his entire company with one line of bad code.”

Many of you would have come across this burning recent news that can prove a setback for anyone. Apparently a man, Marco Marsala, that runs a web hosting company, mistakenly deleted his entire company by running a destructive code, rm -rf. He wrote on a forum that he was trying to fix a bug and ran a bash script on all servers and ended up accidently deleting all his company data. He was now stuck and didn’t know what to do.

Horrible, isn’t it! But this is not the only one instance.

Most of you would have seen the comic movie, Toy story 2. The former Chief Technical Officer of Pixar, Oren Jacob, who was a technical director for the movie shared his experience. He mentioned that at one point when the movie was in creation, they discovered that the movie was being deleted off of the company’s servers after an erroneous command was executed, erasing two months and hundreds of man-hours worth of work. It was then remade putting in a lot of effort in the remaining months in hands to meet its release date. You can read more about this here, http://thenextweb.com/media/2012/05/21/how-pixars-toy-story-2-was-deleted-twice-once-by-technology-and-again-for-its-own-good/.

Accidents can happen, but we need to have a solution in hand that makes us stand still and hold back even in the worst cases of storms. In both the above situations, what could have helped to settle the panic situation when the data was lost? What could have actually brought back the lost data? It is a backup and recovery plan in place.

In today’s data-centric world, the most crucial element in any organisation or enterprise is data. Hence, it is extremely necessary to secure the data and to ensure that it does not gets lost. To protect the data, we need to have a data backup and recovery plan in place.

In the coming topics, we will discuss and understand the purpose of having a backup and recovery plan in place, the processes and methods that help us in implementing the backup and recovery operations and various considerations that we need to take into account when we plan for backup and recovery.

Let us begin with understanding the purpose of having a backup plan in place.

3.1.2 Backup Purpose

A **backup** can be understood as a copy of the production data that has been created and retained entirely for recovering the lost, deleted, or corrupted data.

Data backup is an insurance plan and it is a kind of disaster recovery that should always be a part of any disaster recovery plan. Backing up the data can protect against data loss caused by any reason, such as accidental loss of data, hardware failures, database corruption and even in the case of a natural disaster. With a solid backup and recovery plan in place, we can overcome and recover from all of these. But, if there is no backup and recovery mechanism in place, we are left with nothing to fall back on.

As the businesses and regulatory demands for data storage, retention and availability grow, backing up an ever-increasing amount of data arises as a challenge for the organisations. Adding to that, organisations also need to accomplish a backup plan that costs less and utilises minimum resources.

Organisations need to ensure that the right amount of data is at the right place at the right time. Appropriate backup technologies, recovery and retention requirements for data and application must be evaluated to ensure the successful implementation of the backup and recovery solutions. All such solutions must facilitate quick and easy recovery from backups and archives, as per the business requirement.

It is the job of an administrator to ensure that backups are performed and then stored in a secure location.

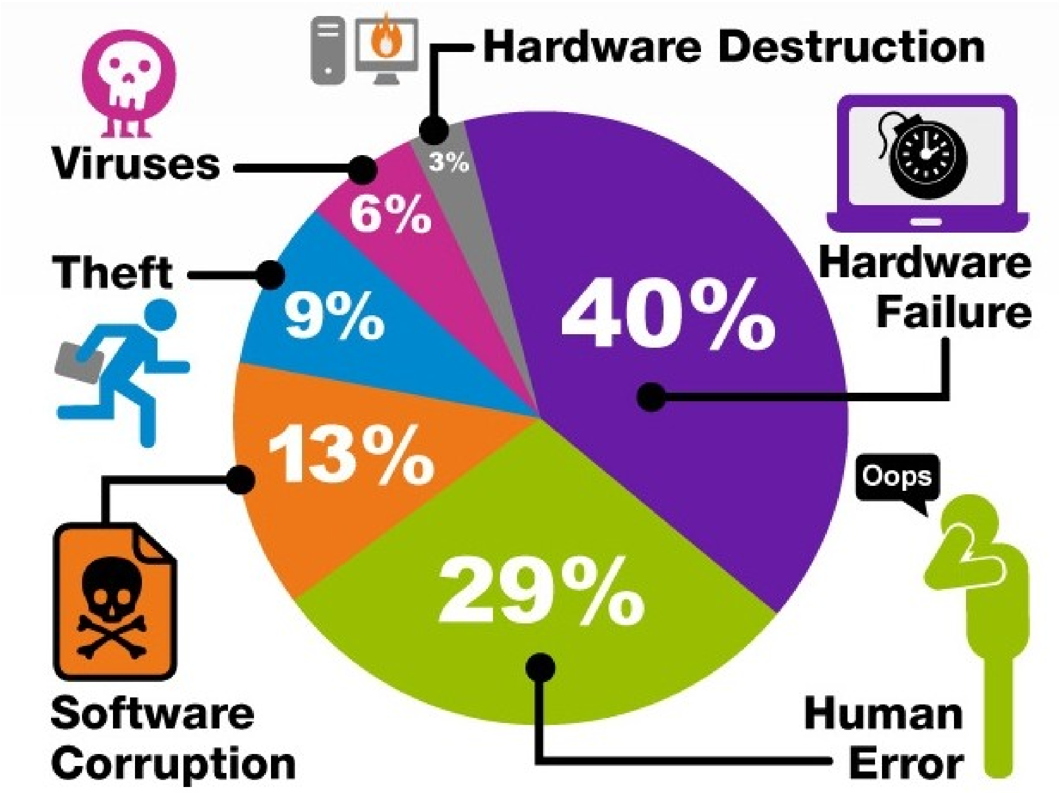


Figure 3.1.1: Reasons for Data Loss

Although there can be many reasons that gives us a purpose to have a backup plan in place, we can broadly categorise the backup purposes in three major categories:

- Disaster recovery
- Operational backup
- Archival

Let us discuss each of these in detail.

(i) Disaster Recovery

Planning for disaster recovery is an integral part of any business strategy. It is becoming more prevalent as network outages and security breaches have emerged out as more common threats.

To address disaster recovery needs, backups need to be performed. Backup and disaster recovery may be not directly interchangeable terms but they have been converging. Disaster recovery is not possible without backup in the first place. Disaster recovery is having the tested wherewithal for the restoration of system and making it run as soon as possible, including the associated data.

When the primary site is incapacitated due to a disaster, then the backup copies are used for restoring the data at an alternate site. Organisations use different backup strategies for disaster recovery, based on Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO and RTO are one of the most important parameters of disaster recovery. They provide guidelines to the organisation for choosing an optimal data backup plan.

In simple words, RPO defines the point in time until when the business process's recovery can tolerably proceed, keeping in mind the volume of data lost in that interval. RTO is the amount of time and a service level taken by a business, within which the business should be restored to avoid unacceptable consequences associated with a break in continuity.

The backup media is shipped and stored at an offsite location, after a tape-based backup method is used as a disaster recovery strategy. When required, these tapes can be recalled for restoration.

(ii) Operational Backup

With every business transaction and operations taking place, data in the production environment tend to change. Operational backup is the backup of data at any given point in time. It is required to restore data in the unfortunate event of a data loss or logical corruptions that may take place during routine processing. Majority of data restoration requests in most of the organisations fall under this category.

For example, it is possible for a user to delete an important file or e-mail accidently, or for a file to become corrupted. In all such cases, data can be restored using the operational backup.

Operational backups are created for the active data in production with the help of incremental or differential backup techniques.

In an incremental backup, only the data that has changed since the last backup is backed up. We can also say that an incremental backup is the backup of latest changes since the last backup. In a differential backup, the data is preserved and only the difference in the data since the last backup is saved. We will read more about these two techniques later in the topic Backup Granularity.

(iii) Archival

Backups are also performed to address the archival requirements of businesses. Even though content-addressed storage (CAS) has emerged as a primary solution for archiving data, small- and medium-sized enterprises still use traditional backups for long-term preservation of e-mail messages, transaction records and other business-related records that are required for regulatory compliance.

CAS is a mechanism of providing fast-access to the data that is not expected to be updated, or is a fixed content, by providing it a permanent place on the disk. It makes data retrieval easy and straightforward as it stores the data in such a way that the stored data can neither be duplicated nor modified. In CAS, the retrieval of the data is made on the basis of its content and not its storage location.

Apart from addressing the three purposes, disaster recovery, operational requirement and archival, backups also serve as data protectors against any kind of data loss due to any physical damage of a storage device, virus attacks, or software failures. Backups can also be used to safeguard the data against accidents, such as accidental deletions, intentional data destruction, or data theft.

Self-assessment Question

1) Which of the following are the reasons for performing a data backup? Choose all that apply.

   a) Data theft
   b) Software corruption
   c) Accidental deletion of files
   d) Archiving data

3.1.3 Backup Considerations

In selecting and implementing a specific backup strategy, prime consideration should be on the amount of data loss and the downtime that a business can withstand in terms of RTO and RPO. The next thing to be considered should be the retention period. You have already read in Module 1 Chapter 2 that a retention period defines the duration for which a business should retain the backed up data. Some data can be retained for years and some only for few days or weeks.

For example, the backed up archival data may be stored for a longer period of time than the backed up operational recovery data.

It is also important to consider the backup media type, based on data accessibility and the retention period and the granularity of backups. Backup granularity is the level of detail used for characterising the backup data. We will discuss more about backup granularity in the next topic.

When developing a backup strategy, it is equally important to analyse and decide about the most appropriate time for performing the backup. It is good to decide on a time when the production operations are not going on so that the work is not disrupted. Similarly, the location and time for the data restore operations must also be considered in advance. You also need to take into consideration the characteristics of the files being backed up and the data compression that can influence the backup process.

Location for data backup and the number and size of files are also important when considering for data backup. They have the potential to affect the backup process.

Location is an important consideration for data backup. Many organisations have numerous heterogeneous platforms that support complex solutions. Imagine a data warehouse environment that uses backup data from multiple sources. Now the backup process must address these multiple sources in terms of transactional and content integrity and the process should be coordinated with all the heterogeneous platforms where the data resides.

File size also has an influence on the backup process. Backing up large-sized files, such as ten 1 MB files, may require less system resource than backing up the same amount of data stored in a large number of small-sized files, such as ten thousand 1 KB files). When a file system comprises of many small files, then the backup and restore operations takes more time.

Similarly, the number of files that needs to be backed up also influence the backup process. ***For example***, consider an incremental backup, where the file system contains one million files with a 10 percent daily change rate. In such situation, there will be almost 100,000 backup entries in the backup catalogue. A backup catalogue contains the table of contents for the backed up data set and information about the backup session. Large number of entries in the file system can adversely affect the performance of the backup and restore process as it is a time-consuming process to search through a huge file system.

The backup performance also heavily relies on the media used for the backup. When there is a large number of small files to be backed up, the time-consuming operations of starting and stopping a tape-based system affects the backup performance. Data compression is widely used in backup systems, as it saves space on the media by compressing the files. Backup devices, such as tape drives, have built-in support for hardware-based data compression. To effectively use the compression techniques, it is important to understand the data characteristics as some data, such as application binaries, do not compress well. Text data gets compressed well and other data, such as JPEG and ZIP files, are already compressed.

In addition to all this, when opting for a backup solution, you must need to consider compatibility, performance, reliability and cost of the backup solution that you are planning to opt and answer the following questions to yourselves:

- **Compatibility**: Will the backup solution support the business infrastructure?
- **Performance:** How quickly and smoothly will the backups complete?
- **Reliability:** Will the backup solution be reliable and the backed up data be available when required?
- **Cost:** How much investment should be made for a backup solution?

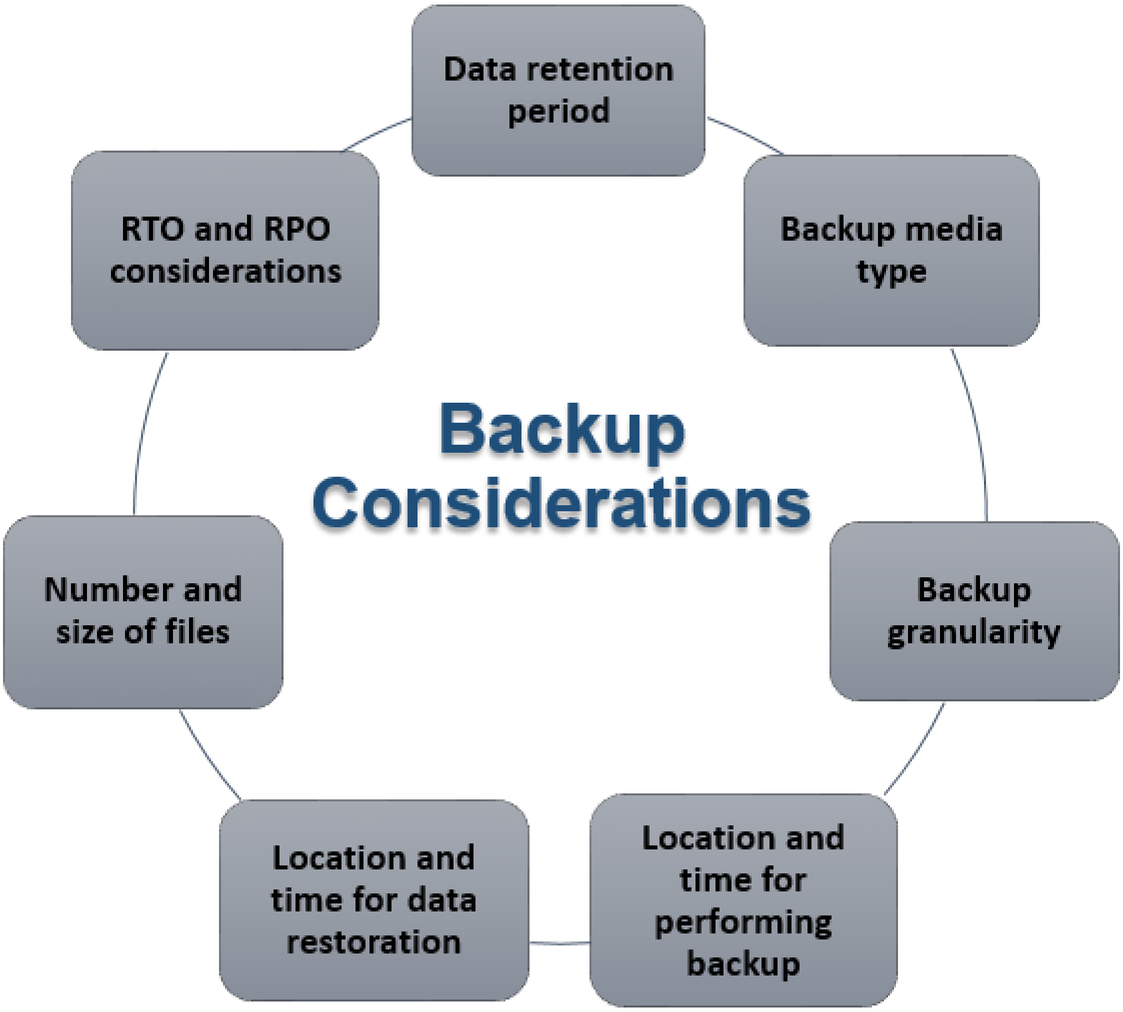

Data retention period
Backup media type
Backup granularity
Location and time for performing backup
Location and time for data restoration
Number and size of files
RTO and RPO considerations
Backup Considerations

Figure 3.1.2: Backup Considerations

Self-assessment Question

2) Which of the following needs to be taken into consideration when planning for a data backup?

a) Size of the files	b) Location of storage
c) Cost of the backup solution	d) Backup granularity

3.1.4 Backup Granularity

Backup granularity, as mentioned earlier, describes the scale or level of detail in characterising the backup data. Increased granularity improves the RPO as the backup process operates, using more discrete granules or increment of data. This minimises the amount of data lost during a system restore. A backup and restore system designed for maximum granularity improves the RPO and significantly, reduces the labour investment needed for a backup administrator.

Backup granularity is dependent on the needs of the business and the required RTO and RPO. On the basis of granularity, backups can be categorised into three types:

- Full
- Incremental
- Cumulative

To meet the backup and recovery requirements, most of the organisations today use a combination of these three backup types. Let us learn about each of these types in detail.

Full Backup

A full backup is the most basic and complete type of a backup operation. As the name implies, it is a backup of the full and complete data on the production volumes at a given point in time. A full backup makes a copy all the data on a secondary storage device, such as a tape. Disk, CD or DVD. It provides a single repository that makes data restoration easy.

Advantages of Full Backup

- The main advantage of performing a full backup during every operation is that a full copy of entire data is available within a single set of media.
- It is also easy to maintain and restore different versions.

Disadvantages of Full Backup

- The main disadvantage of using a full backup is that it takes longer to perform a full backup as compared to other backup types.
- Also, a full backup requires more storage space than others.

Hence, full backups are generally performed periodically. Data centres having a small amount of data or those having critical applications, may opt to run a full backup on a daily basis or on more often regular intervals. Typically, backup operations employ a full backup in combination with either differential or incremental back up.

Incremental Backup

In an incremental backup, only the data that has changed since the last full or incremental backup, whichever has occurred more recently, gets copied. Typically, the modified time stamp on the files is compared to the time stamp of last backup, while performing incremental backup. Backup applications keep a track record of the date and time when a backup operation takes place in order to track the files that got modified after the last backup operation.

Since an incremental backup copies only the modified data since the last backup, it can be run as often as desired, with only the most recent changes getting stored.

Advantages of Incremental Backup

- The advantage of using an incremental backup is that it copies only a small amount of data than copying the entire data and hence it is faster to complete.
- Since, the volume of backed up data is restricted to the changed data, it required lesser media to store the backup.

Disadvantage of Incremental Backup

- The main disadvantage of incremental backup is that it takes longer to restore.

Cumulative Backup

These are also known as differential backups. It is similar to an incremental backup the first time it is performed where it copies all the changed data with respect to the previous backup. However, every time it is run afterwards, it copies all the data that got modified since the last full backup. Hence, a cumulative backup stores more data than an incremental backup on subsequent operations, although far less data than a full backup.

Advantage of Cumulative Backup

- The main advantage of cumulative backups is that it is easy and faster to restore.

Disadvantages of Cumulative Backup

- It takes longer to perform data backup operations than incremental backups.
- It requires more storage space and time than incremental backups, although less than full backups.

When it comes to data restoration, a full backup provides a single repository from which data can easily be restored. In an incremental backup, the process of restoration requires the last full backup as well as all the incremental backups available until the point of restoration. In a cumulative backup, the restoration requires the last full backup and the most recent cumulative backup.

Let us refer to Table 3.1.1 that clearly mentions how the three backup operations work.

Backup Number	Full	Incremental	Cumulative
Backup 1	Full data	-	-
Backup 2	Full data	Changes from backup 1	Changes from backup 1
Backup 3	Full data	Changes from backup 2	Changes from backup 1
Backup 4	Full data	Changes from backup 3	Changes from backup 1

Table 3.1.1 Comparison of the Three Backup Operations

Each backup type works differently as shown in Table 3.1.1. A full backup must be performed at least once. Thereafter, either another full, an incremental or a cumulative backup can be run. The first partial backup performed, which can be either a differential or an incremental backup, backs up the same data. By the third backup operation, the data that gets backed up with an incremental backup is restricted to the changes since the last incremental backup. When you compare, the third backup with a cumulative backup will backup all changes since the first full backup, which was backup 1, in this case.

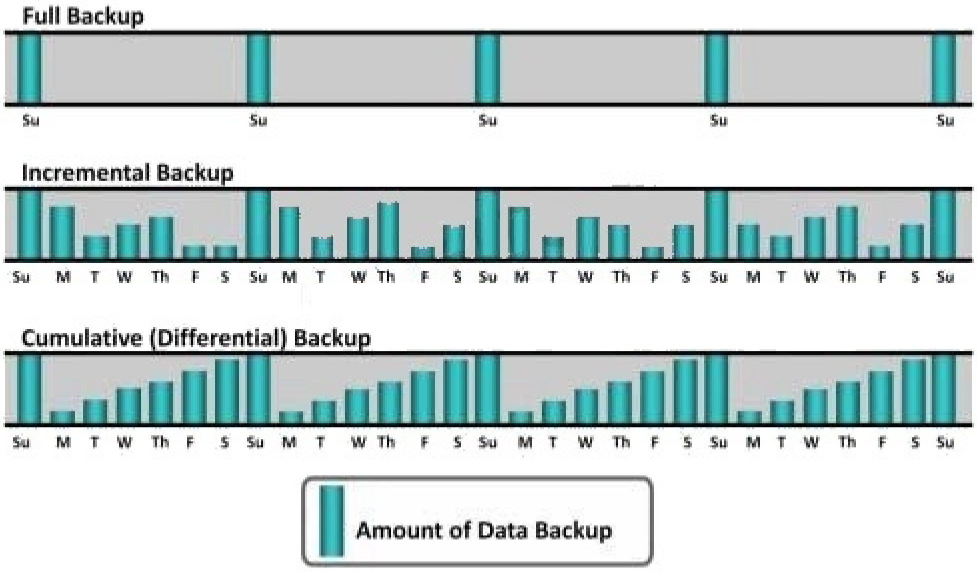


Figure 3.1.3: Types of Backup Granularity

Apart from these three backup types, there is one more kind of backup known as **synthetic** or **constructed full backup**. It is used in implementations where the volume of production resources cannot be exclusively reserved for a backup process for extended periods to perform a full backup.

A synthetic full backup is generally created from the most recent full backup and all the incremental backups that have been performed after that full backup. It enables a full backup copy to be created offline without disrupting the input/output (I/O) operation on the production volume. This frees up network resources to get involved in the backup process and makes them available for other production uses.

Depending on the granularity of the backup, restore operations may vary. Combining the three primary types of backup operations, it is possible to develop a secure approach to protect data. Typically, depending on the size of the business and its data securing needs, one of the following approaches can be used for safeguarding data:

- Full daily
- Full weekly + Cumulative daily
- Full weekly + Incremental daily

Self-assessment Question

3) Which of the following backup techniques takes the longest to perform the backup operations and generally should be performed periodically?

a) Incremental backup	b) Cumulative backup
c) Full backup	d) Differential backup

4) Which of the following backup technique, from its second backup, copies all the data that got modified since the last full backup?

a) Cumulative backup	b) Full backup
c) Incremental backup	d) Synthetic full backup

5) Which of the following backup technique creates a full backup copy offline without disrupting I/O operation on the production volume?

a) Full backup	b) Synthetic full backup
c) Incremental backup	d) Cumulative backup

3.1.5 Recovery Considerations

There is a fair chance that you would like your business to survive any future disaster and any problems that may follow. It is almost impossible to predict what and when the next disaster will take place, but it is easy to stay prepared for it, especially if you have proper and effective backup and recovery mechanisms.

It is important to understand what needs to be taken into consideration when planning for a backup. Two of the major considerations, when trying to achieve a backup strategy, are RPO and RTO. Both the RPO and RTO are two very specific parameters that are closely associated with data backup and recovery. They sound fairly similar, but they are actually quite different.

Understanding RPO

For a business, RPO specifies the time intervals between two backups and defines the tolerance limit of data loss. In other words, we can say that, RPO determines the backup frequency. The main focus of RPO is on the data and on the business's loss tolerance in relation to the data.

RPO can be determined by focusing on the time between data backups and the amount of data that might get lost in between the backups. As part of a business continuity planning, you need to identify the time period the business can afford to operate without that data, before the business starts to suffer.

For example, if an application, ABC, requires RPO of one day, it would require the backup of data at least once every day. Or in a simpler example, imagine that you are working on a very important and lengthy presentation and the computer crashes in between. All the data written after you last saved the presentation will get lost. Imagine the time period you can tolerate having to try to recover, or, maybe, rewrite that lost content.

That time, for you, becomes RPO. It should become the indicator of how often you back up your data, or in this case, save your presentation. If you realise that your business can survive without incurring losses for, maybe, five to six days in between the backups, then the RPO for your business should be five days, the shortest time between backups.

The retention period for a backup is also derived from an RPO that has been specified for operational recovery. ***For example***, users of application, ABC, might want to restore the application data from its operational backup copy, created a month ago. The retention period for the backup is determined by this. Hence, based on operational recovery requirements, the RPO for application, ABC, can range from one day to a month. However, the organisation can choose to retain the backup for a longer period of time, based on internal policies or external factors.

When you specify short retention periods for backups, it may not be possible to recover all the data required for the requested recovery point. Some data may be older than the retention period.

Longer retention periods can be defined for all the backups. It makes it possible to meet any RPO within the specified retention period. But having this requires a huge storage space as well, which can lead to higher costs. Hence, it is very important to perform an analysis of all the restore requests in the past and the allocated budget to correctly define the retention period.

Understanding RTO

After a disaster has struck, RTO is the target time that is set for the recovery of the data and business activities. The aim is to calculate how quickly the recovery can be made. This calculation can guide to the kind of preparation that needs to be implemented and the overall budget that needs to be assigned for business continuity.

For example, if the RTO is identified as 10 hours, it means the business with systems down can only survive for this period of time. It raises an alarm and requires a high-level of preparation along with higher budget for the quick recovery of systems. However, if the RTO is identified as 15 days, then, probably, you can budget less and invest in less-advanced solutions for data backup.

To meet the desired RTO and to minimise the recovery time, the business can choose a variety and combination of different backup solutions. The kind of backup media that should be used gets highly influenced with RTO in a backup environment.

For example, in multiplexing, data is sent from multiple clients to a single tape drive. Hence, recovery from data streams that are multiplexed in tapes takes longer to finish than the recovery made from tapes with no multiplexing.

Keeping the recovery constraints in mind, the businesses usually perform more full backups than actually required. When performing the restoration from tape media, it requires several tapes to completely recover the system. With a full backup, recovery can be made with a lower RTO and fewer tapes.

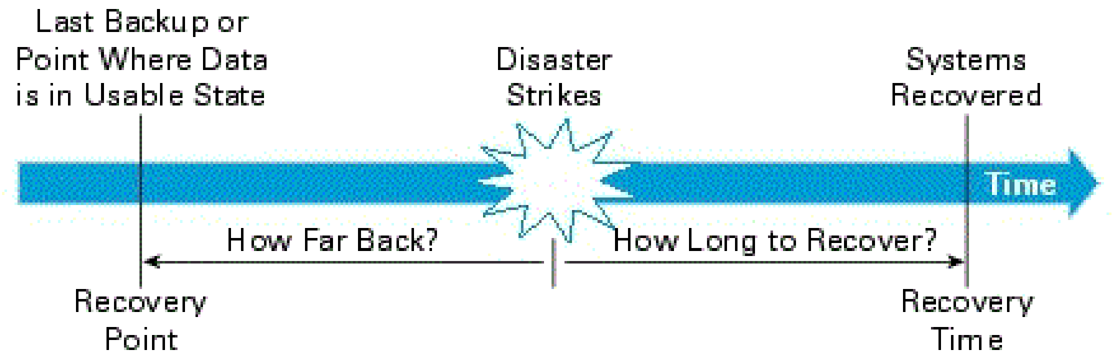


Figure 3.1.4: RTO and RPO

Difference between RTO and RPO

Although, both RPO and RTO are closely associated with backup and recovery, the main difference between the two is their purpose. Where RPO has its focus majorly on data and on the business's ability to deal with data loss, RTO is generally large scale and focuses at the complete business and the involved systems.

RPO and RTO may be different, but both should be considered when opting for a backup plan for business continuity.

Self-assessment Question

6) Which of the following primarily focuses on data and the business's loss tolerance in relation to data?

a) RTO	b) RPO
c) Both RTO and RPO	d) None of these

3.1.6 Backup Methods

Now that we have understood the purpose of performing backup and recovery operations, we need to know the backup methods. The two methods deployed for backup based on the state of the application when the backup is performed are:

- Hot backup
- Cold backup

Hot Backup

A **hot backup** is also known as a dynamic backup. It is performed when the application is up and running and the data is actively accessible to users and may currently be in the state of being updated. It is performed in situations where it is not possible to shut down the database. This is facilitated by **database backup agents**. These agents help perform the backup while the database is active and live; however, these agents usually affect the overall application performance and slows down the performance.

It is a challenging task to back up the online production data as it gets actively used and changed.

While the backup operation is in progress, the operating system locks the open files and doesn't allow it to be copied unless the user closes it. During the backup process, the backup application retries to copy the open files at certain intervals. When an open file is closed by the user during a backup operation, the retry becomes successful and it gets copied. The maximum number of retries that a backup operation can perform can be configured based on the backup application.

However, this method cannot be considered robust as in some environments certain files are always meant to be open. ***For example***, in a garments business, the file that maintains the log of inventory cannot be closed as it has to record the details of every ongoing transaction.

In such situations, the backup applications provide **open file agents**. These open file agents directly interact with the operating system to enable the creation of consistent copies of open files. However, in some environments, the use of open file agents is also not sufficient.

For example, a database consists of many files of different sizes that occupies several file systems. To ensure a consistent database backup, all the files need to be backed up in the same state. That does not necessarily mean that all files need to be backed up at the same time, but they all must be synchronised so that the database gets restored with consistency.

Advantage of Hot Backup

- As the hot backup performs the backup operation on the active data, there are no issues of downtime and users can carry on with their work as usual.

Disadvantages of Hot Backup

- Since the data being backed up may be in the state of being updated, if the data gets altered while the backup is in progress, the resulting copy might not match the signal state of the data. In order to perform a recovery, the inconsistency must be resolved.
- It takes longer to perform the backup operation than the cold backup.
- The application performance is slowed down.

Cold Backup

A **cold backup** is also known as offline backup. It is performed when the database is offline and the applications are not active and hence, not accessible for updating. The cold backup helps in taking the consistent backup of the database by requiring the database to remain inactive during the entire backup operation.

Advantages of Cold Backup

- A cold backup is the safest way to perform data backup as it avoids the risk of copying any data that could be in the process of being updated.
- It is faster than a hot backup.

Disadvantage of Cold Backup

- Although the cold backup is safe to perform, it involves downtime as users cannot access the database while it is being backed up.

In environments where the impact of downtime from a cold backup or the performance resulting from a hot backup is unacceptable, there a **point-in-time (PIT) copy** method is deployed. A PIT is used as a method of backup and data protection and is a copy of a storage volume, file, or database as they appear at a given point in time. When required, the data from the most recent PIT copy can be restored.

A pointer-based PIT copy consumes only a fraction of the storage space and can be created very fast. It is implemented in a disk-based solution whereby a virtual logical unit number (LUN) is created. This LUN hold the pointer to the data stored on the saved location. While the PIT is created, the database is frozen or stopped for a moment. The PIT copy is then mounted on a secondary server while the backup occurs on the primary server.

It is not sufficient to back up only the production data for recovery, in order to ensure consistency. Certain attributes and properties attached to a file, such as permissions, owner and other metadata, are also required to be backed up. These attributes are equally important as the data itself and must be chosen to be backed up to ensure consistency.

For a successful recovery, it is critical to backup the boot sector and partition layout information as well. When performing a disaster recovery, a bare-metal recovery (BMR) backs up all the metadata, system information, application configuration to ensure a full system recovery. BMR builds the base system, which includes partitioning, file system layout, applications, operating system and all the relevant configurations. BMR recovers the base system first, before starting the recovery of data files. Some BMR technologies can also recover a server onto dissimilar hardware.

Self-assessment Questions

7) Which of the following backup methods should be used in an environment where the database cannot be shutdown to perform a backup?

a) Cold backup	b) PIT copy
c) Hot backup	d) BMR backup

8) Which of the following directly interacts with the operating system to enable the copying of open files?

a) Database backup agents	b) Point-in-time copy
c) Bare-metal recovery	d) Open file agents

3.1.7 Backup Process

Now that we have understood the methods of backup, let us focus on understanding how the backup system works. A backup system uses the client/server architecture in which there is one backup server and multiple backup clients. The backup operations are managed by the backup server and it also maintains the backup catalogue. As mentioned earlier in this chapter, a backup catalogue contains information about the backup process and backup metadata. To perform the backup activities, the backup server receives backup metadata from the backup clients.

The data gathering for backup is done by the backup clients and the backup server depends on the backup clients for the same. The backup clients can either be local to the server or they can reside on any other server, presumably to back up the data visible to that server.

In a backup environment, a storage node is a host that control the backup devices. The storage node is responsible for writing data to the backup devices. Generally, the storage node is integrated with the backup server and both the storage node and the backup server are hosted on the same physical platform.

The storage node's host platform attaches a backup device directly with itself. At some instances, you may come across the backup architecture referring the storage node as the media server. This is because the storage node connects to the storage device. Storage nodes can be used for consolidating the backup servers and hence, plays an important role in the backup planning. Policies that are defined in the backup server, such as time of the day for completion of an event, also defines the basis for the backup process.

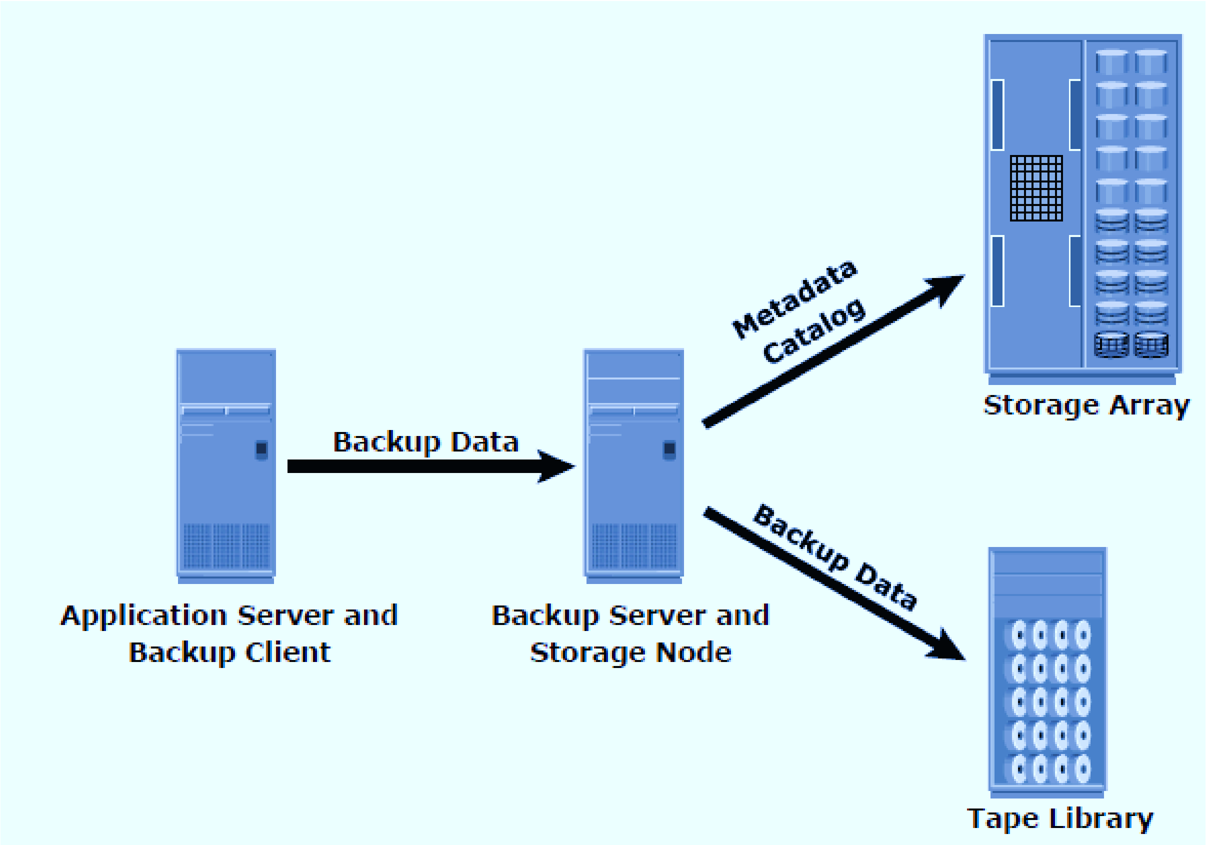

Metadata Catalog
Storage Array
Backup Data
Backup Data
Application Server and Backup Client
Backup Server and Storage Node
Tape Library

Figure 3.1.5: Backup Architecture and Process

The backup server initiates the backup process by sending a request to one of the backup clients. Based on the instructions of the request, the backup client sends its metadata to the backup server and also sends the data to be backed up on the appropriate storage node. This metadata is written on the metadata catalogue by the backup server. The backup client also sends the data to the storage node and the storage node writes the data to the storage device.

The storage node closes the connection to the backup device, after all the data is backed up. The backup completion status is written by the backup server to the metadata catalogue.

The backup catalogue and the log files contains all the information of the backup and can help in generating reports, such as the amount of data backed up, the number of completed backups, the number of incomplete backups and the types of errors that may have occurred during the backup. Reports can be customised depending on the specific backup software used.

Did You Know?

Backups can also be initiated by a client server.

Self-assessment Questions

9) In a backup process, which of the following maintains the backup catalogue?

a) Backup client	b) Backup server
c) Storage node	d) Storage array

10) Which of the following is manages the backup devices and is also known as the media server?

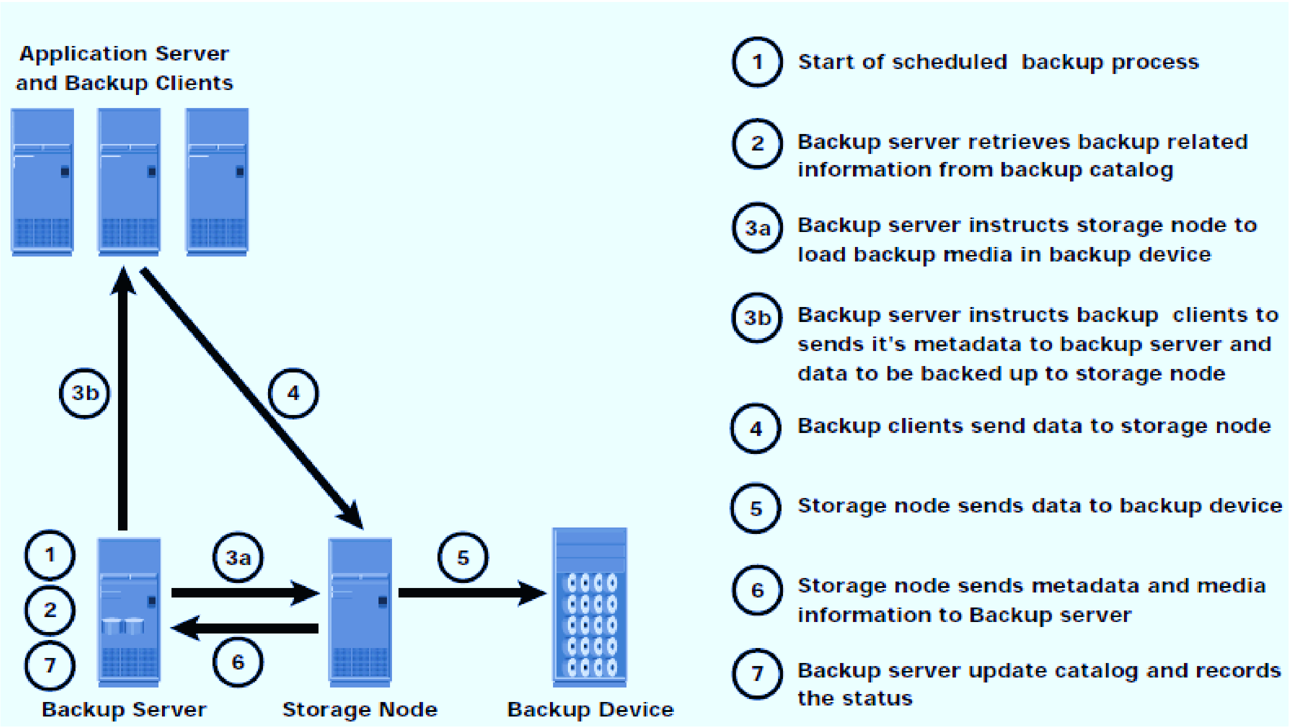
a) Backup server	b) Application server
c) Storage node	d) Backup client

3.1.8 Backup and Restore Operations

Backup Operations

When a backup process gets initiated, along with that, significant network communications also takes place between the different backup infrastructure components. The backup process for different client is initiated by the backup server, based on the backup schedule configured for each of them. ***For example***, the backup process for a set of clients may be scheduled to start at 1400 hours every day.

In a backup configuration, the backup server coordinates the backup process with all the components. Let us refer to the Figure 3.1.6 to understand it better.



1 Start of scheduled backup process

2 Backup server retrieves backup related information from backup catalog

3a Backup server instructs storage node to load backup media in backup device

3b Backup server instructs backup clients to sends it's metadata to backup server and data to be backed up to storage node

4 Backup clients send data to storage node

5 Storage node sends data to backup device

6 Storage node sends metadata and media information to Backup server

7 Backup server update catalog and records the status

Figure 3.1.6: Backup Operation

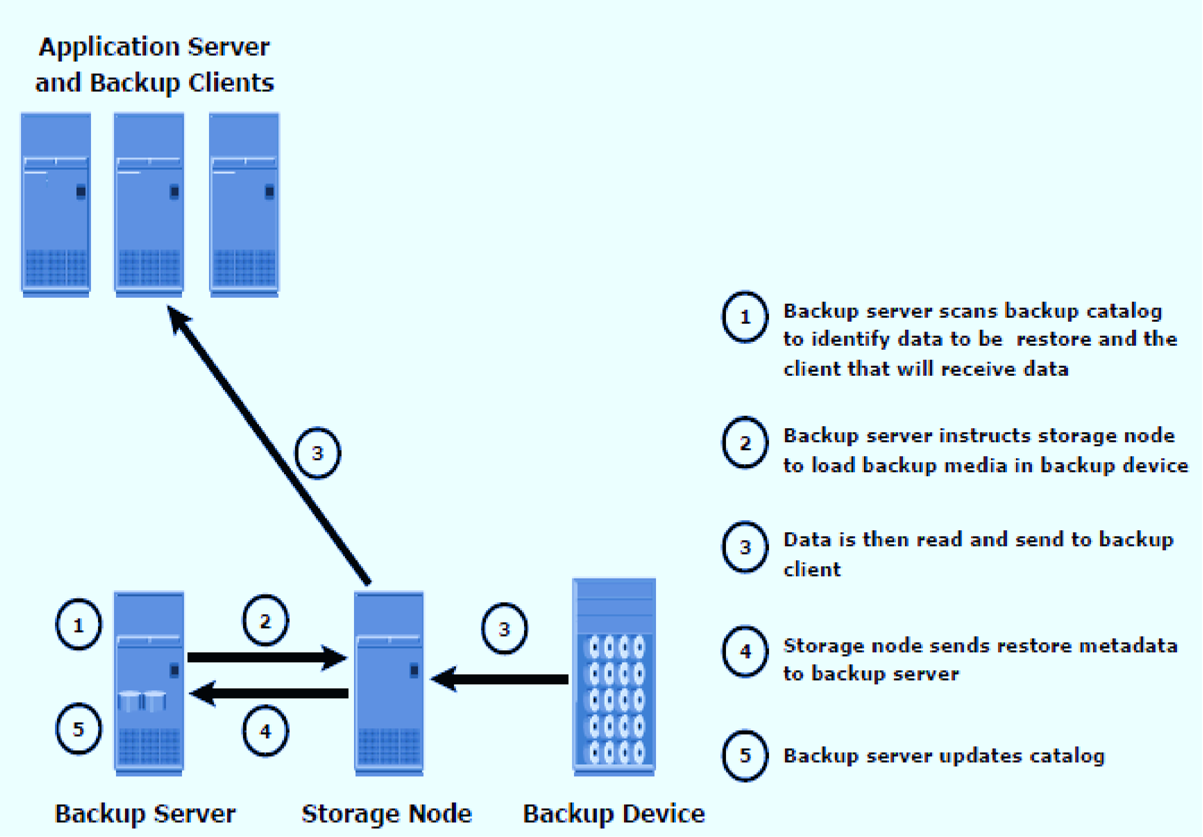
The information about the backup clients to be contacted and the storage nodes to be used in a backup operation is maintained by the backup server. It also retrieves the backup-related information from the backup catalogue. Based on the information, the backup server instructs the storage node to load the appropriate backup media into the backup devices. On the other hand, it also instructs the backup clients to start the scanning of data, package it and send it over the network to the assigned storage node.

After receiving the instructions from the backup server, the storage node sends the metadata to the backup server in order to keep it updated about the backup media used for the backup operation. The backup catalogue keeps on getting updated by the backup server continuously as and when it gets a new information. After the data gets backed up, it can be restored as per the requirement.

Restore Operations

A restore process needs to be manually initiated. Some backup software uses separate application for data restoration and only the administrator has the rights to access these restore applications.

Let us refer to the Figure 3.1.7 to understand a restoration process.



Application Server and Backup Clients
1 Backup server scans backup catalog to identify data to be restore and the client that will receive data
2 Backup server instructs storage node to load backup media in backup device
3 Data is then read and send to backup client
4 Storage node sends restore metadata to backup server
5 Backup server updates catalog
1
2
3
3
4
5
Backup Server
Storage Node
Backup Device

Figure 3.1.7: Restore Operation

When the administrator receives the restoration request, it opens the restore application in order to view the list of backed-up clients. When the administrator is in the selection process of the client for which the restore request has been made, it also needs to identify the client that needs to receive the restored data. While the data can get restored on the same client for whom the restore request has been made, it is also possible that it gets restored on a different client as well.

Thereafter, the administrator selects the data to be restored and based on RPO, it also selects the specific point in time when the data neds to be restored. The restore application must be in communication with the backup server, as all of this information is fetched from the backup catalogue.

The administrator initiates the restore process by selecting the data that needs to be restored. The backup server then identifies the appropriate media that is to be mounted on the backup devices, with the help of appropriate storage nodes. Then the data is transferred to the client that has been identified to receive the restored data.

Some restorations get successfully accomplished by recovering only the requested production data. ***For example***, the recovery process of a spreadsheet is completed when the specific file is restored. In database restorations, additional data such as log files and production data, are a must to be restored. This is to ensure application consistency for the restored data. In these cases, the RTO needs to be extended because of the additional steps in the restoration process.

Self-assessment Questions

11) Which of the following maintains information about the backup clients to be contacted and the storage nodes to be used in a backup operation?

a) Backup server b) Storage node
c) Backup catalogue d) Storage array

12) In the restore operations, which of the following contains the information regarding the data to be restored along with its specific point in time of restoration?

a) Backup server b) RPO
c) Storage node d) Backup catalogue

Summary

- A backup is a copy of the production data that has been created and retained entirely for recovering the lost, deleted, or corrupted data.

- The backup purposes can be broadly categorised into three major categories, disaster recovery, operational backup and archival.

- RPO defines the point in time until when the business process's recovery can tolerably proceed, in terms of the volume of data lost in that interval.

- RTO is the amount of time and a service level taken by a business, within which the business should be restored to avoid unacceptable consequences associated with a break in continuity.

- Data retention period, backup media type, backup granularity, location and time for performing backup, location and time for data restoration, number and size of files and RTO and RPO consideration are some of the important backup considerations.

- Backup granularity describes the scale or level of detail in characterising the backup data. On the basis of granularity, backups can be categorised into three types, full, incremental and cumulative.

- In an incremental backup, only the data that has changed since the last full or incremental backup, whichever has occurred more recently, gets copied.

- A cumulative backup copies all the data that got modified since the last full backup.

- Two of the major considerations, when trying to achieve a backup strategy, are RPO and RTO.

- A hot backup is also known as a dynamic backup. It is performed when the application is up and running and the data is actively accessible to users and may currently be in the state of being updated.

- A cold backup is also known as offline backup. It is performed when the database is offline and the applications are not active and hence, not accessible for updating.

- A backup system uses the client/server architecture in which there is one backup server and multiple backup clients. The backup operations are managed by the backup server and it also maintains the backup catalogue.

Terminal Questions

1. What is the purpose of performing disaster recovery, operational backup and archival?

2. Discuss in detail about the cold and hot backup methods with respect to their usage.

3. Discuss in detail why do we need to have a backup of the data.

Answer Keys

Self-assessment Questions	
Question No.	**Answer**
1	a, b, c, d
2	a, b, c, d
3	c
4	a
5	b
6	b
7	c
8	d
9	b
10	c
11	a
12	d

Activity

Activity Type: Offline **Duration:** 30 Minutes

Description:

Provide a situation to perform backup and recovery.

Ask the students to identify various backup and recovery techniques to apply for the given situation.

Case Study

Simco IT is an IT company that uses tape as its primary backup storage media. Full backups are performed every Sunday. Incremental backups are performed Monday through Saturday.

The environment contains many backup servers that back up different groups of servers.

During the backup process, the e-mail and the database applications need to be shut down. Due to the decentralised backup environment, recovering the backup data is often compromised. There are too many tapes that need to be mounted to perform a full recovery in case of a complete failure and the time needed to recover is too lengthy.

The company would like to deploy an easy-to-manage backup environment. They want to reduce the amount of time the e-mail and database applications are unavailable and reduce the number of tapes required to fully recover a server in case of a failure.

1. Propose a backup and recovery solution to address the company's needs.
2. Justify how your solution ensures that their requirements will be met.

Bibliography

e-References

- Singh, J. (2008). Understanding RPO and RTO. *Druva Blog*. Retrieved from http://www.druva.com/blog/understanding-rpo-and-rto/

- *The difference between RTO and RPO*. (2014). *Techadvisory.org*. Retrieved 2 July 2016, from http://www.techadvisory.org/2014/07/the-difference-between-rto-and-rpo/

- *What is differential backup? - Definition from WhatIs.com*. (2016). *SearchDataBackup*. Retrieved 2 July 2016, from http://searchdatabackup.techtarget.com/definition/differential-backup

- *Full Backup | Types of Backup*. (2012). *Typesofbackup.com*. Retrieved 2 July 2016, from http://typesofbackup.com/full-backup/

Image Credits

- Figure 3.1.1: http://tbyd.ca/wp-content/uploads/2015/05/Causes-of-data-loss-pie-chart.jpg

- Figure 3.1.3: http://cdn.aiotestking.com/wp-content/uploads/e10-001-v1/10.jpg

- Figure 3.1.4: http://sqlserver-dba.co.uk/wp-content/uploads/2011/09/RTO-and-RPO1.gif

- Figure 3.1.5: Information Storage and Management: Storing, Managing and Protecting Digital Information

- Figure 3.1.6: Information Storage and Management: Storing, Managing and Protecting Digital Information

- Figure 3.1.7: Information Storage and Management: Storing, Managing and Protecting Digital

External Resources

- Somasundaram, G. & Shrivastava, A. (2009) *Information storage and management* - Storing, managing and protecting digital information. *Indianapolis, Ind.: Wiley Pub.*

- Dufrasne, B., Eriksson, R., Martinez, L., & Kalabza, W. (2014). *IBM XIV Storage System Architecture and Implementation* (9th ed.). International Business Machines Corporation.

Video Links

Topic	Link
Backup considerations	https://www.youtube.com/watch?v=-oRdxh1sCR0
Backup architecture	https://www.youtube.com/watch?v=DliUzzgk4pk
RTO and RPO	https://www.youtube.com/watch?v=mpFbrEATs4s

Notes: