

Recovery

INFO-6081 – Monitoring & Incident Response

Learning Outcomes

- Incident or Disaster
- Disaster Recovery
- Restoring Data
- Backup and Recovery
- Backup Types
- Backup Methods
- Backup Targets

Incident or Disaster

- Recovery can be an action of incident response, or an action of Disaster Recovery (DR)
- In some cases, incidents that have been detected by the IR team escalate to the level of disaster
- Should this occur, the incident response process is no longer equipped to handle the effective and efficient recovery from the loss and the disaster recovery plan should be activated
- Disaster recovery describes the steps an organization must take to recover from a natural or man-made disaster

Disaster Recovery

- If an organization's resources are crippled by an attack, such as that experienced by the shipping giant Maersk in 2017 when they were the victim of the NotPetya ransomware, the incident would be categorized as a disaster (man-made)

Some examples of natural disasters include:

- Fire
- Flood
- Earthquake
- Lightning
- Landslide or Mudslide
- Tornado or Hurricane
- Tsunami
- Electrostatic Discharge (ESD)
- Dust Contamination
- Excessive Precipitation

Incident Response – Recovery

- When an incident has been contained, and the organization is in control of its assets, recovery operations can begin
- The first task of recovery is to assess the damage that was caused and adjust the scope and scale of the recovery to match
- If evidence may be required for legal proceedings, this must be identified before recovery commences
 - If evidence is uncovered during forensic analysis or during recovery operations, it is imperative that the individuals performing the operation are trained to handle the material in a way that does not violate its value as evidence

Restoring Data

- Many organizations confuse the roles of data recovery and incident response
- Data recovery plays a critical role in IR, but data recovery alone is simply not enough
- The IR team must be aware of the organization's backup strategies, and should be involved in the recovery process
- Some applications have more than one path to restore data, and an IR team needs to be aware of the correct procedures for each type

Backup and Recovery

- A backup is an additional copy of production data that is created for the purpose of recovering lost or corrupted data
- Most organizations generate and maintain large volumes of fixed data
- After a period, this content is rarely accessed; however, regulatory requirements may dictate that the data is retained for several years
- Backups are performed to serve one of three purposes:
 - Disaster Recovery
 - Operational Recovery
 - Archival

Backup and Recovery – Disaster Recovery

- When considering backups for disaster recovery, the backup copies are used to restore data at an alternate site when the primary site is incapacitated due to a disaster
- Regarding recovery, two terms are often used:
 - **Recovery Point Objective (RPO)**
 - RPO describes the amount of data that can be “lost” within the BCP’s maximum tolerance
 - RPO specifies the backup frequency
 - **Recovery Time Objective (RTO)**
 - RTO describes the duration of time within the service level agreement, by which point the process or service must be restored

Backup and Recovery – Operational Recovery

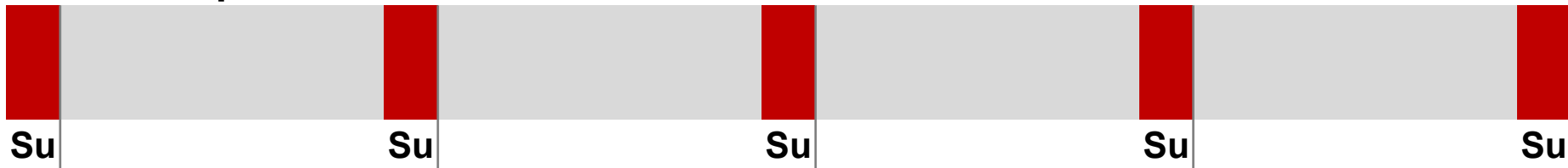
- Data in a production environment is constantly changing with each new transaction
- If a system or database suffers from logical corruption or data loss, and operational recovery will restore the system to a consistent state
- Most recovery actions fall within the operational recovery category

Backup and Recovery – Archival

- Data archiving describes the process of moving data sets that are no longer needed from primary to secondary storage
- Data is often retained on secondary storage long term to meet regulatory requirements
- Data archives are also subject to backup; however, the frequency of archive backups may be reduced

Backup Granularity

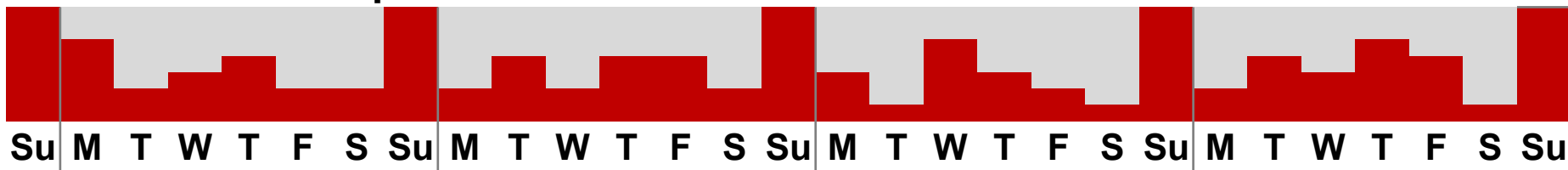
Full Backup




Differential Backup





Incremental Backup



Backup Schedule

Full: 

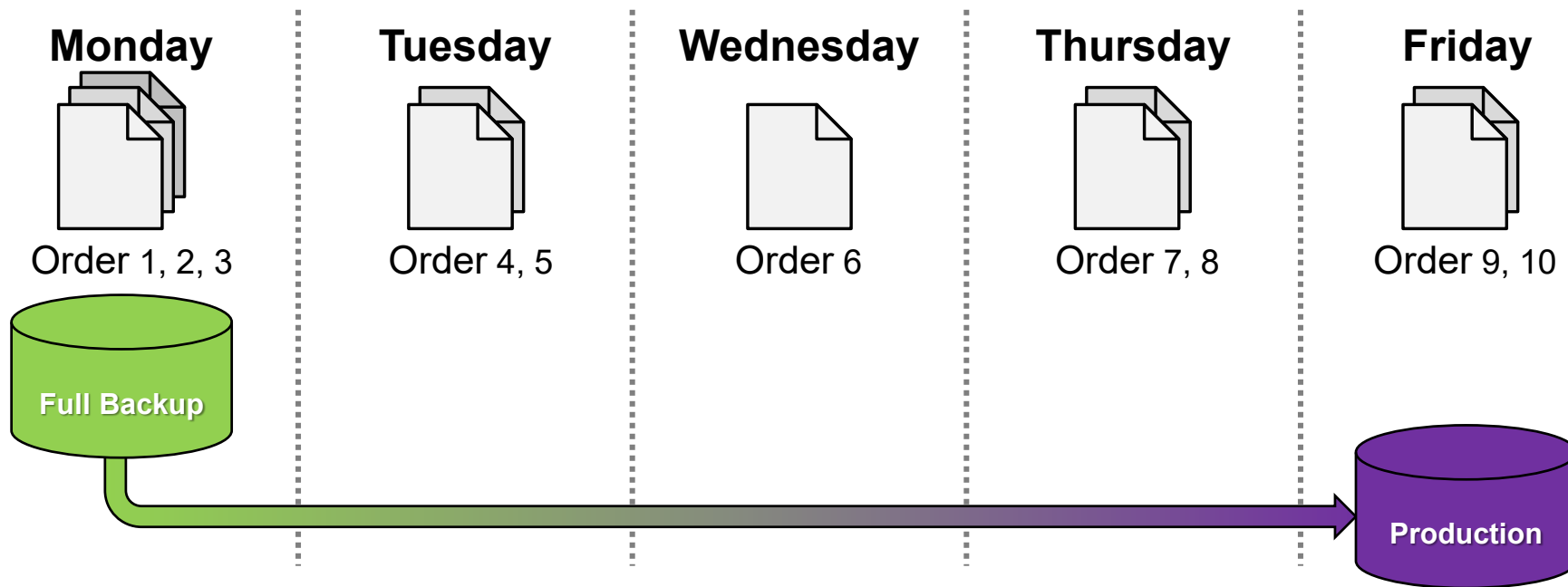
Differential: 

Incremental: 

November						
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

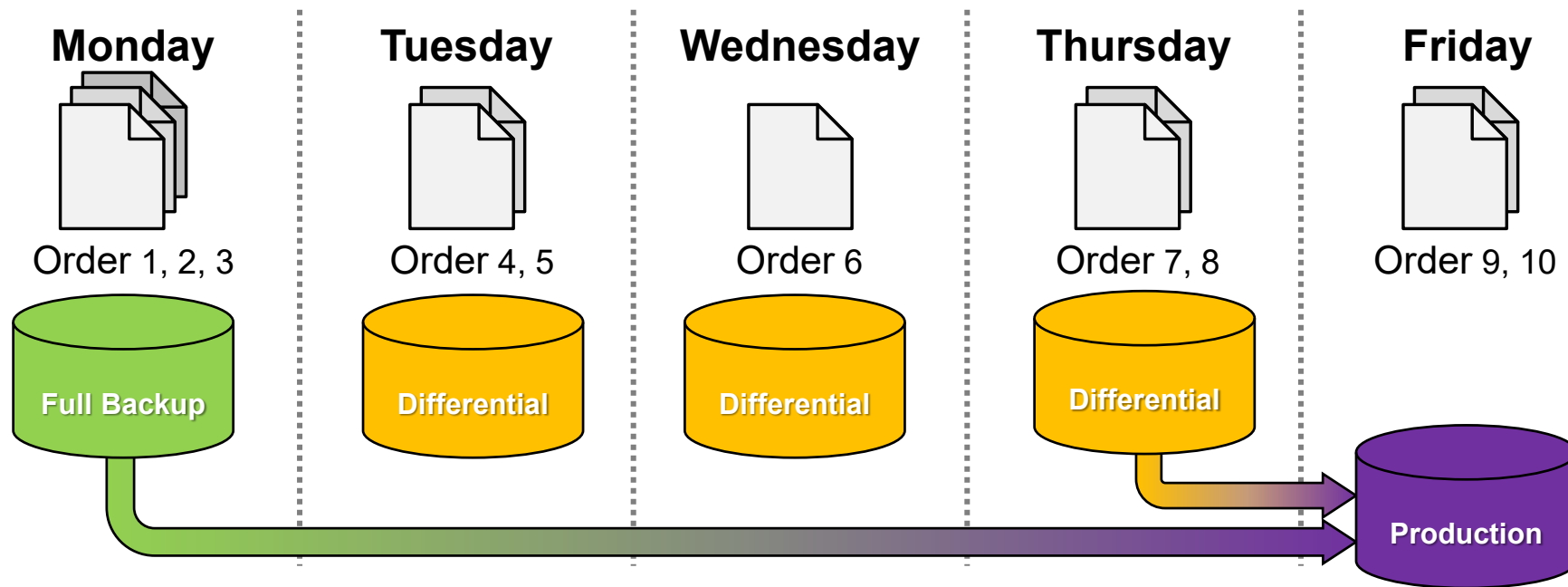
Backup Types – Full Backup

- Restoring from a full backup is the simplest form of restoration
- Only one restore operation is required to revert to the recovery point objective
- May require additional data entry before business resumption



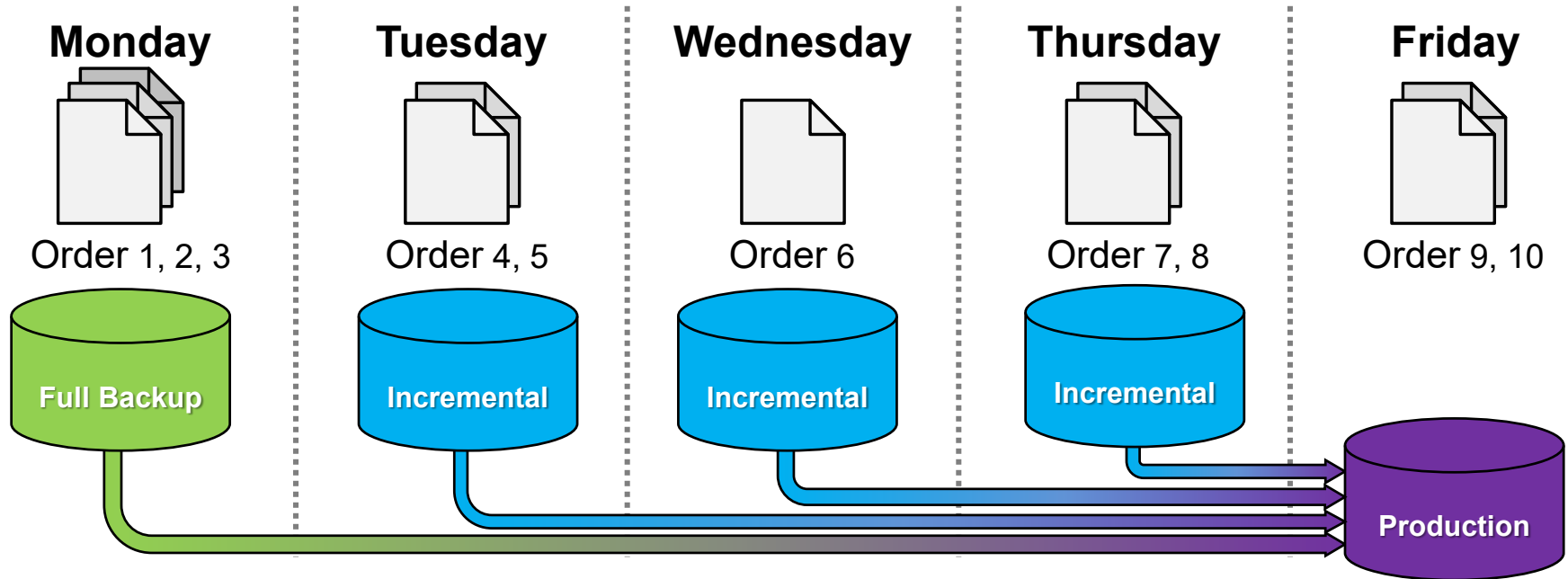
Backup Types – Differential Backup

- Files that have changed since the last full backup are saved
- Two restore operations are required to revert to the recovery point objective
- Minimal data entry required before business resumption



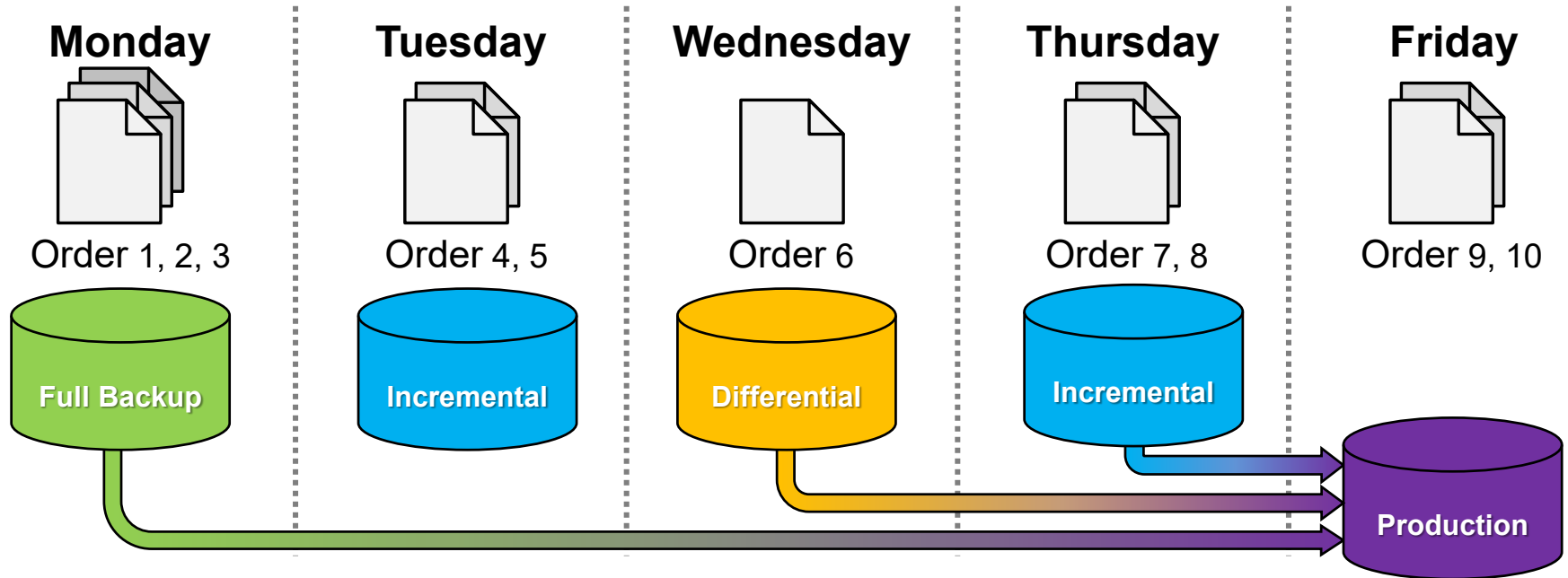
Backup Types – Incremental Backup

- Files that have changed since the last backup are saved
- Many restore operations may be required to revert to the recovery point objective
- Minimal data entry required before business resumption



Backup Types – Combination Solution

- Combines backup strategies for most efficient use of time and backup size
- Multiple restore operations may be required to revert to the recovery point objective



Backup Types – Other Considerations

Additional backup types include:

- **Synthetic Full Backup**

- Data from the last full backup is logically combined with differential and incremental backups to create a single restore point

- **Continuous Backup**

- A service monitors files or file systems for changes, and saves a copy of any file that has been modified
- The backup process is transparent to the end user, but restore options are often available to the user
- Microsoft's Shadow Copy Service provides some of the features of a continuous backup solution

Backup Methods

The two backup methods are:

- **Hot**

- The application is running at the time the backup is taking place
- Also known as an online backup
- May require an open file agent to backup open files

- **Cold**

- The application or system is shut down at the time the backup is taking place
- Also known as an offline backup

Backup Methods – Database Systems

- Backing up database systems is more complex than using an open file agent
- A database can be comprised of many file of various sizes spread across multiple file systems
- It is imperative that a backup is consistent and, while all files may not need to be backed up at the same time, they must be synchronized so that the database can be restored with consistency
- Transactional logs are often a component of database backups, allowing transactions to be added or removed from the database

Backup Targets

There are various targets available for backups including:

- **Tape**

- Traditional storage media
- LTO-10 will offer 48 TB or storage per tape

- **Optical Drives**

- Blu-ray discs can store up to 100 GB per disc

- **Hard Disk Drives (HDD)**

- Fast data transfer speeds available

- **Flash Storage**

- Ranges from slow (USB thumb drives) to fast (Solid State Drives)

- **Cloud Storage**

- Normally tape or HDD supported by a third party

Summary

- In some cases, an incident will escalate to the point that it is reclassified as a disaster
- Disaster recovery describes the steps an organization must take to recover from a natural or man-made disaster
- Data restoration may be required in both incident response and disaster recovery
- Backups are performed to serve one of three purposes: Disaster Recovery, Operational Recovery, Archival
- Backup Types include Full, Differential, Incremental, Synthetic Full, Continuous
- Backups can be taken either online or offline
- Backups can be stored on many different media types, all of which have advantages and disadvantages

References

- Whitman, M. E., Mattord, H. J., & Green, A. (2014). Chapter 8: Incident Response: Recovery and Maintenance. Principles of incident response and disaster recovery (2nd ed.). Australia: Course Technology Cengage Learning.
- Whitman, M. E., Mattord, H. J., & Green, A. (2014). Chapter 9: Disaster Recovery: Preparation and Implementation. Principles of incident response and disaster recovery (2nd ed.). Australia: Course Technology Cengage Learning.

References

- Gnanasundaram, S., & Shrivastava, A. (2012). Chapter 10: Backup and Archive. Information storage and management: storing, managing, and protecting digital information in classic, virtualized, and cloud environments. Indianapolis: John Wiley & Sons.