Backup Strategy for IT Disaster Recovery Plan Using Active Data Guard and NetBackup

Muhammad Iqbal[1], Lulu Chaerani Munggaran[2]
[1]Department, Gunadarma University, Depok, West Java, Indonesia-16424
[2]Department, Gunadarma University, Depok, West Java, Indonesia -16424
Email address: mhdiqbale@gmail.com, lulu@staff.gunadarma.ac.id

***Abstract*— *Based on The National Agency for Disaster Countermeasure (BNPB) Indonesia, until December 4th, 2018 there were 1134 disasters that occurred in various regions in Indonesia. This natural disaster reinforces the fact that good plans are needed long before a natural disaster will occur again for either a country, a province, a city or an organization / company. One of insurance company in Indonesia has a lot of labor data with several employment guarantee programs. To maintain the business continuity of company, a disaster management plan is needed to ensure all data of a company are safe and usable. The company has several database servers stored both in the Data Center (DC) and Disaster Recovery Center (DRC). Each database server has the main backup method, but the backup files are stored in the same site. Therefore, an alternative backup method should be implemented and put them outside the DC and DRC sites. One alternative database backup method is using tape. In this study, the author will implement the database backup method through a combination of Active Data Guard and NetBackup applications as a risk mitigation of damage or loss of data due to natural disasters and to complete the IT DRP document as guidelines standards of the business continuity management of the company.*

***Keywords*— *Backup, business continuity plan, database, disaster recovery plan, netbackup, oracle data guard, replication.*

I. INTRODUCTION

The Business Continuity Plan (BCP) is a comprehensive plan that helps an organization / company prepare for various types of emergencies. BCP is a methodology used to create and validate plans to maintain a sustainable business operation before, during, and after disasters and disruptive events [1]. A BCP generally begins with a Business Impact Analysis (BIA) that identifies an important function in which BCP then documents how to maintain these functions when a disaster occurs. BCP helps continue business even after a breakdown occurs. Business must remain active during a crisis, if a company closes its operations for daily or then this company will face losses and must be closed [2]

The Disaster Recovery Plan (DRP) provides details on how to recover a system or several from a disaster. BCP keeps important functions running during disasters, while DRP has a focus on identifying how to restore the system [3].

Information Technology DRP compiled in this study is based on ISO/IEC 20000, which is an international standard that serves as a guideline for the alignment of IT services with the business processes. It precisely defines core requirements concerning the processes of service continuity and availability management, the documents and records that should be produced and retained by the service continuity and availability management process. The insurance company have mandatory programs which are workplace accident security, old age security and death security. Employers also can gradually enroll their workers into the pension security. These social security program have many sensitive data. IT DRP is a part of the Operational Guidelines Standards of the Business Continuity Management (BCM) of the company, containing guidelines for officials / employees and related parties both internal and external (providers / vendors) that support the company's services, to be used in the event of an emergency that causes the operation to be abnormal, not even functioning at all.

In this study, IT DRP is designed for one of insurance company di Indonesia that is needed as a control for operational risk mitigation related to information technology such as corrupt databases, application errors, disconnected network connections to the worst possible risks, namely damage to hardware and disruption of operational activities both at headquarters and branches. Thus, so that this purposed backup strategy can serve as a guideline for all ranks of the IT Directorate in implementing operational recovery in the event of a disaster.

II. PROBLEM IDENTIFICATION

A database is a whole piece of information that is integrated and logically connected, the data system and the connections between them are stored [4]. A backup plan is part of the DRP. Data recovery cannot be done if there is no data backup. Policies in backing up important data must be in a company where it has been regulated in terms of conditions for identifying and determining media and storage retention. The risk of damage and data loss remains even though a company has a DC and DRC site. Therefore, a Standard Operational Procedure (SOP) is needed for operational recovery due to natural disasters.

III. RELATED WORKS

A database management system (DBMS) is a computer application program designed for the efficient and effective storage, access and update of large volumes of information [5]. Many research methods have been carried out to improve database availability. Logical standby database is used by standby database to update by SQL statement with the aim to achieve zero failover [6]. Oracle Data Guard is used on the physical standby database by sending redo logs to ensure data consistency as a solution to disaster recovery solutions [7]. The use of Oracle Data Guard is also done in achieving zero downtime and modifying the TNS file to prevent users from connecting to the primary database after a failure on the primary system [8]. The implementation of IP failover by using keepalived on the redhat server will make the client connection quickly change to standby database replication using the Virtual Reduction Routing Protocol (VRRP), where standby database server replication uses Oracle Data Guard technology [9]. Use of Bacula software with the full backup-restore method in handling DRP [10].

TABLE I. Related works.

No.	Author	Year	Research
1	Singh and Singh	2013	Maintaining Client Connectivity and Zero Failover Using Oracle Data Guard Grid Computing.
2	Kaur and Kaur	2014	Achieving Zero Failover Using Logical Standby Database in Oracle Data Guard.
3	Prabhudas, Surekha, and Ramesh	2016	Maximum Availability Architecture of Oracle Servers.
4	Awasthi, Kumar, and Grag	2017	Data Handling using Oracle Data Guard by the Transfer of Log Sequence.
5	Handrini, Kurniawan, and Widjajarto	2018	Disaster Recovery Strategy *Menggunakan Software Bacula dengan Metode* Full Backup-Restore

IV. METHODOLOGY

The proposed method in preparing backup copies of data in and outside the DC and DRC sites as shown in Figure 1.

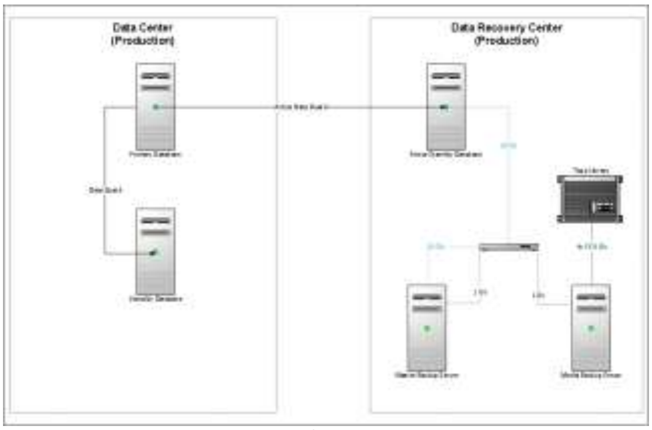

Fig. 1. General architecture of database backup and replication

The recovery phase as Figure 2 is used for designing IT DRP. Mirroring is the main technique used in planning to rebuild business operational development [11]. Database mirroring technology can be used to increase database availability, business continuity, disaster recovery, and performance even if the distances between servers are located far apart by sending transaction log records directly from one server to another standby server [12].

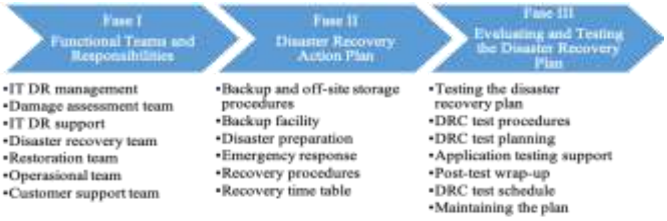

Fig. 2. The recovery phase in a phase approach [13]

One of the technologies in replicating databases is to use Oracle Data Guard, which functions to manage, monitor, maintain, and monitor one or more standby databases to protect the company data from failure, disaster, errors, and damage. Oracle Data Guard (ODG) is used to replicate the main database to the standby database. ODG can manage and maintain more than one standby database to convert to database production to survive when disasters occur.

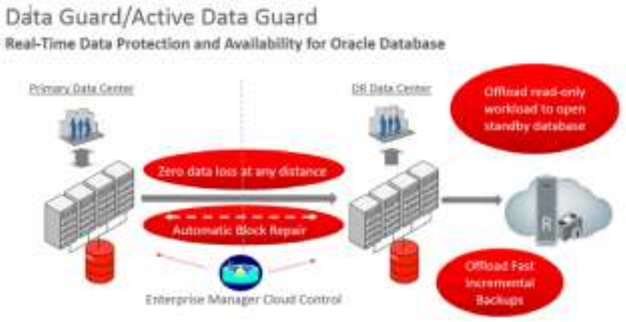
Data Guard/Active Data Guard
Real-Time Data Protection and Availability for Oracle Database
Primary Data Center
DR Data Center
Offload read-only workload to open standby database
Zero data loss at any distance
Automatic Block Repair
Enterprise Manager Cloud Control
Offload Fast Incremental Backups

Fig. 3. Architecture of Oracle Active Data Guard

Figure 3 shows the architecture of oracle Active Data Guard. Steps to build an active standby database using Active Data Guard:

- Primary Server Setup
- Standby Server Setup (Manual)
- Start Apply Process
- Test Log Transport

There are two basic methods of configuring ODG, physical standby database and logical database standby. Standby physical databases are equivalent to the main database while logical standby databases have a logical scheme that is the same as the main database but may have different physical objects, such as additional indices. Active Data Guard (ADG) is a technology that provides real-time data replication at the physical level. Oracle ADG propagates through transactional oracle logs (redo log or archive log). However, one of the limitations of the ADG is that it cannot filter the replicated data [14].

Data Guard provides three different modes for adjusting cost, availability, performance, and data protection. Each mode uses a specific transfer method and defines the Data Guard configuration behavior if the main database loses contact with the standby database.

NetBackup is an application that provides complete and flexible data protection solutions for various platforms.

Platforms include Microsoft Windows, UNIX, and Linux systems. The topology of implemented NetBackup as shown in Figure 4. During the backup/archive process, the client sends backups of data across the network to the NetBackup server. The NetBackup server manages the type of storage specified in the backup policy [15].

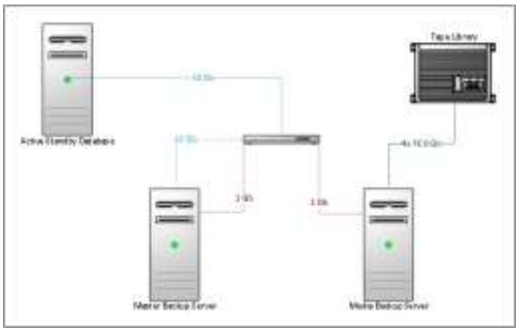

Fig. 4. Implemented NetBackup topology

V. RESULT AND DISCUSSION

The basic function of Oracle Data Guard is to keep a copy of the database that is synchronized as standby, to make provisions, if the main database cannot be accessed by end users [18]. Data Guard transports logs from primary to the standby machine, and then apply them on the standby machine to keep the standby database consistent with the primary database.

Build active standby database:

1. Backup primary database and restore to standby server.
2. Cancel the media recovery on physical standby:
   ```
   SQL > alter database recover managed standby database cancel;
   ```
3. Open the database:
   ```
   SQL > alter database open;
   ```
4. Start media recovery with read-time log apply:
   ```
   SQL > alter database recover managed standby database disconnect;
   ```
5. Check the database status:
   ```
   SQL > select name, open_mode from v$database;
   ```

Confirm the physical standby database open mode as read only with apply.

The data may be frequently updated by the user, including updating, insertion, deletion, and appending that also called Data Manipulation Language (DML) process, to ensure storage correctness under dynamic data update is hence of paramount importance. However, solution to resolve data lost issue by backup with data storage on cloud or external server [16]. Recovery Manager (RMAN) is a backup and recovery tool made by Oracle, where these tools can protect data effectively and efficiently [17]. NetBackup is a Symantec's backup software used to make backups of data on enterprise-class. NetBackup is also used RMAN in processing backup. Implementation of Symantec NetBackup 7.6 located at the Data Center marked with installation Master Backup. There is one client that has been installed for Oracle database backup. Backup device used is Symantec Appliance 5230 which is functioned as a media server one the dedupe disk and Quantum Tape Library with fiber channel connection.

One phase that have to be implemented while preparing the document of IT DRP is Disaster Recovery Action Plan:

1. Backup and off-site storage procedure
2. Disaster preparation
3. Emergency response
4. Recovery procedures
5. Recovery time table

A. Backup and off-site storage procedure

All backup files should be duplicate to tape periodically. The tapes that contains backup images are taken outside the Data Center.

- Backup strategy
  a. The Information Services tape library contains all the required tape sets for the daily, weekly, monthly, and yearly. This device is a Quantum LTO6 Tape Library.
  b. Offsite Backup tapes are rotated on a two weeks cycle taken form Data Center using a dry box.
  c. All Offsite Backup tapes are stored at dry cabinet out site DC/DRC.

- Backup sets
  a. Differential backup, contains image backup files, data files changed since the last full backup.
  b. Full backups, contains all image backup files of a database in the Data Center.
  c. Offsite backups, contains duplication of full backup stored on external disk.
  d. Semi-annual backups, contains another Full Backups three times a year in April, August, and December

- Backup tape schedule
  a. Differential backup, scheduled on Sunday to Thursday which runs every midnight.
  b. Full backup, scheduled on Friday nights.
  c. Offsite backup, scheduled every Friday the fourth weeks.
  d. Semi-Annual Backup 1—April.
  e. Semi-Annual Backup 2 – August.
  f. Semi-Annual Backup 3 – December.

B. Disaster preparation

The minimum steps needed in order to ensure the Data Center can fully recover from a disaster.

TABLE II. Categories of High Availability Solutions [19]

Platinum	• *Zero outage for Platinum Ready Applications* • *Zero data loss*
Gold	• *Comprehensive HA and Disaster Protection* • *Zero or near-zero data loss*
Silver	• *High Availability (HA) for Recoverable Local Outages* • *Data protection as of last backup*
Bronze	• *Basic Service Restart* • *Data protection as of last backup*

- The disaster plan must be kept up to date and everyone on the recovery team must be notified of the change of plan and drilled for the tasks assigned to them.

- Offsite storage must be completed every month to ensure clean, orderly storage and the correct backup is in external storage.
- The fire system in the computer room must be stored every year. The head of the department must realize the improvement plan and develop alternative data while the recovery is in progress.
- Emergency Data Center phone number of the person concerned.
- Procedures and waiting times for decision and communication equipment must be determined.
- All computer members must agree on appropriate emergency and evacuation procedures.

C. Emergency response

The basic actions that need to be taken in the event of a disaster situation.

- The IT DRM members or designee should be notified as soon as possible.
- The disaster recovery team should be notified and assembled as soon as reasonable under the circumstances.
- Team members should assess damages to their individual areas of expertise. The recovery procedures should include an estimated timeline for restoration of specific services based on the service priority. The estimate can include alternative interim solutions for specific services during the reconstruction of permanent solutions.
- Team members should advise the Director of IT DRM as to the extent of damage and recovery procedures necessary so that the decision to move the Data Center can be made after the assessment of the damage to the current facility has been determined.
- Pertinent vendors should be contacted and negotiations should be made for the delivery of equipment, delivery time should be noted. All department heads should be informed of the decision and given an estimated time for the return to either full or degraded services.
- Each member of the disaster recovery team should supervise his or her own area of expertise.
- The computer facility should be safe and secured.

D. Recovery Procedures

The lower the RTO and RPO, the better an IT DRP is, directly proportional to the increase in costs required [20]. Recovery from a complete failure to a degraded mode of services may be necessary. In this case it may be possible to bring up individual departments on a priority basis.

- The decision to operate in a degraded mode and the order in which departments are to be brought back into service should be made by the Director of IT DRM in consultation with team members of IT DR Support.
- An inventory of the status of existing equipment and files should be compiled.
- The leader of IT DR Management should coordinate the move of facility to Disaster Recovery Center.
- Vendors should be contacted to initiate delivery of replacement equipment to the Data Center backup facility. The estimated time of delivery should be noted.
- A new offsite storage facility should be located and used immediately, if necessary.
- All facility systems should be verified operational at this time.
- Systems should be tested and loaded as soon as the vendors release them to the Data Center.
- Helpdesk, Network Management Team, Database Management Team, System Administrator and Applications Software Team should be prepared to install and or setup their individual function in the appropriate order.
- All department heads should be made aware of progress on a regular basis.
- Existing safety and emergency procedures at the backup facility should be examined for their adequacy as a computer room.

E. Recovery time table

The following timetable is estimated

- First hour, convene the disaster recovery team, ascertain the extent of the damage and evaluate potential consequences, notify department heads, contact vendors, discuss options.
- Second hour Release formal communication to the business units and stakeholders. At the disaster site, carry-out a safety inspection, inventory status of existing equipment and files, make a full evaluation of the damage, provide detailed accounting for insurance claims, and retrieve vital documents and reusable equipment.
- Third to fifth hour, switch over or fail over the database system or application and network system

TABLE III. Backup database time estimate

Type	Backup Location	Time elapsed	Input	Output
Backup	Internal Primary Database Server	14.07 hours	21 TB	4.4 TB
Backup	Internal Active Physical Standby Database Server	10.82 hours	21 TB	4.4 TB
Backup	Symantec NetBackup (internal disk)	13,45 hours	21 TB	21 TB
Backup	Symantec NetBackup (duplication to tape)	36,01 hours	21 TB	21 TB (4 tape)

Backup and restore time estimate as shown on Table III and Table IV. Specification of database server DC and DRC:

- Operating system: Oracle Solaris 11.2 SPARC
- Database version: Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
- Server: Oracle M6-32
- VCPU: 256

Memory: 1.94 TB (128 GB for PGA, 1.25 TB for SGA)

TABLE IV. Restore database time estimate

Type	Backup location	Time elapsed	Backup files
Restore	Primary Database Server	18 hours	4.4 TB
Restore	Symantec NetBackup	29 hours	23 TB

Disaster recovery testing scenario of database server as shown on Table V.

Specification of database server DC and DRC:

- Operating system: Oracle Solaris 11.2 SPARC
- Database version: Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
- Server: Oracle M6-32
- VCPU: 256
- Memory: 1.94 TB (128 GB for PGA, 1.25 TB for SGA)

Fujitsu PY RX2540 and Symantec NetBackup Appliance 5230 is used for backup solution server.

TABLE V. Disaster recovery testing scenario

Scenario	Location	Time elapsed	Method
Switch over	DC to DRC or DRC to DC	15 minutes	Oracle Data Guard
Failover	Internal Active Physical Standby Database Server	15 minutes	Oracle Data Guard
Restore	Symantec NetBackup	29 hours	RMAN

VI. Conclusion & Future Research

The technology should not be expensive and should enable businesses to complete use out of their Disaster Recovery investments. Oracle Data Guard is not the only solution available today that meets all these needs but is one of the easy and best to use, combining with NetBackup make the backup of our data to be effective, efficient, and secure. This is for support IT DRP document and as a basis for determining the value of a company's RPO and RTO. It is clear that the historical approaches of data protection are not likely to meet the demands of the next generation data centers. In order to solve the problem of data growth, and to meet the aggressive SLAs laid down by regulatory mandates, the company will continue to adopt new technologies such as disk-based data protection, deduplication, virtualization, snapshots, and replication. There are many tools nowadays that can be used for better and faster backup solution. The key is the lower RPO and RTO, the better an IT DRP.

References

[1] Snedaker, S. *Business Continuity and Disaster Recovery Planning for IT Professionals*. Elsevier: Waltham, MA, 2014.

[2] Jorrigala, V. "Business Continuity and Disaster Recovery Plan for Information Security," M.S. thesis, St. Cloud State University., Minnesota, 2017.

[3] Gibson, D. *Managing Risk in Information System*. Jones & Bartlett Learning, Burlington, 2015.

[4] Ayyavaraiah, M. and Gopi, A. *Database Management System.* Horizon Books, Delhi, 2017.

[5] Prabhjot and Sharma, N, "Overview of Database Management System. *International Journal of Advanced Research in Computer Science*," 8(4), pp. 362-369, 2017.

[6] Kaur, E.M. and Kaur, E.M, "Achieving Zero Failover Using Logical Standby Database in Oracle Data Guard. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(12), pp. 394-397, 2014.

[7] Awasthi, R.M., Kumar, S. and Garg R. "Data Handling Using Oracle Data Guard by the Transfer of Log Sequence," *International Journal for Research in Applied Science & Engineering Technologi (IJRASET)*, 5(4), 1241-1246, 2017.

[8] Singh, G. and Singh, S. "Maintaining Client Connectivity and Zero Failover Using Oracle Data Guard Grid Computing," *Journal of Global Research in Computer Science*, 4(7), pp. 5-9, 2013.

[9] Prabhudas, J., Surekha, T.L. and Ramesh M. "Maximum Availability Architecture of Oracle Servers," *International Journal of Innovations in Engineering and Technology (IJIET)*, 7(3), pp. 454-460, 2016.

[10] Handrini, E.A., Kurniawan, M.T. and Widjajarto, A. (2018), "Disaster Recovery Strategy Menggunakan Software Bacula dengan Metode Full Backup-Restore," *E-Proceeding of Engineering*, 5(2), pp. 3190-3197, 2018.

[11] Sinha, P.K. and Sinha, P. *Information Technology: Theory and Practice*. PHI Learning Private Limited, Delhi, 2016.

[12] Narang, R. *Database Management Systems*. PHI Learning Private Limited, Delhi, 2011.

[13] Mohamed, H.A.R. "A Proposed Model for IT Disaster Recovery Plan," *I. J. Modern Education and Computer Science*, 4, pp. 57-67, 2014.

[14] Baranowski, Z., Pardavila, L.L., Blaszczyk, M., Dimitrov G. and Canali, L. (2015). Evolution of Database Replication Technologies for WLCG, 664(4), 1-9.

[15] *Symantec NetBackup Getting Started Guide Release 7.6*, Symantec Corporation: Mountain View, 2013.

[16] Vora, S.B. and Anandache, J.G. "Data Backup on: Cloud Computing Technology in Digital Libraries Perspective," *Journal of Global Research in Computer Science*, 5(12), pp. 12-16, 2014.

[17] Kuhn, D. *Oracle RMAN for Absolute Beginners*. Apress, California, 2014.

[18] Baransel, E. and Nassyam B. *Oracle Data Guard 11gR2 Administration*. Packt Publishing Limited, Birmingham, 2013.

[19] Jovanovic, Z. "Business Continuity Options for Oracle Technology Solutions," *International Journal of DIGITAL TECHNOLOGY & ECONOMY*, 1(1), pp. 33-41, 2016.

[20] Alhazmi, O.H. "Computer-Aided Disaster Recovery Planning Tools (CADRP)," *International Journal of Computer Science & Security (IJCSS)*, 9(3), pp. 132-139, 2015.