Disaster recovery planning with distributed replicated block device in synchronized API systems

K Budiman*, F Y Arini, and E Sugiharti

Computer Science Department, Mathematics and Science Faculty, Universitas Negeri Semarang, Indonesia

*Corresponding author: kholiq.budiman@mail.unnes.ac.id

Abstract. System backup can’t be a good solution without planning. Secure data backup planning will prevent more data loss. The Comprehensive Exam is a system to conduct a comprehensive exam and test score management, which is also carried out with the Computer-Based Test. The two systems are connected, these are running with a data-based application programming interface (API) synchronization on two different servers. Two servers running simultaneously with the synchronized API. Special methods of solving this problem are needed to back up supported information systems and computer-based tests. Disaster Recovery is a term for recovery and resumption. A disaster recovery plan is a plan to improve information technology (IT) infrastructure from other disasters that endanger the information infrastructure. One method of recovering business processes is to restore the data backup itself. Data backup is one of the important elements, the data backup method will be applied is the disk mirroring method, which is making a permanent backup from the main data center, data backup will be provided a real-time backup using the Distributed Replicated Block Device (DRBD) concept. In our research concluded automatically synchronizes implementation backup data using the DRBD concept.

1. Introduction
Continuity is an important requirement in businesses, many examples show the disruptions in information technology services have a large impact on business functions cause losses impact on the reputation and income of the organization [1]. Therefore, we need an information system design supports the sustainability of a system to continue working to support an organization, also it needs an infrastructure which can run an information system properly. Without good infrastructure, the system will not run smoothly and sustainably. To make good computer infrastructure service we need carefully planning, it also requires building infrastructure planning to pay attention to threats that will occur. Research conducted by Budiman, Tony and Amie also propose the construction and development of information systems must be in harmony and in accordance with the strategic direction of the organization (company) so there is no failure in development [2]. Threats that will occur include natural disasters, viruses, ransomware, and others. According to Bhattacharya et al. (2017), several issues on data recovery is inconsistency or loss of data. But with periodic backups and good backup planning, it can suppress data loss and overcome other threats [3].

The Comprehensive System is a system carried out to order comprehensive exams and also value management of exams which are also carried out with Computer-Based Tests. The two related systems are running with a data-based API synchronizing that runs on two different servers can be seen in Figure
1. So if one server encounter an interruption, both servers will be interrupted too, and can be seen in Figure 2.

The two servers running in parallel with the Synchronizing API cause obstacles in making backups from the system side as well as the database, therefore special methods are needed to perform a system backup between comprehensive information system and computer-based test. This backup method represents a Disaster Recovery. In building disaster recovery need good planning, so the disaster recovery can be a solution when the server is on interruption.

2. Theoretical background

2.1. Data center

The data center is a collection of facilities that not only provide data storage services, but data center provides a variety of supporting services such as communication equipment, supporting equipment to connect servers to the internet and various equipment to control other infrastructure. To run the data center facility, it needs electricity. According to Ammar 2018, a number of challenges are facing the design of secure datacenter environments, namely, fulfilling high throughput requirements; support for low latency applications [4]. One of the most important challenges is how the Electric Power role in enabling the management of the data center to run continuously [5].

2.2. Disaster Recovery Plan

In computer processing systems, application downtime effect in financial losses for companies. The downtime is caused by some disaster, according to Sahi, Lai and Li 2016 types of disaster that may cause major damage to any system: (1) natural disasters, such as flood, earthquake, and volcano, (2) man-made disasters, such as cybercrime and technological terrorism, and (3) technological accidents, such as infrastructure failure, and transportation failure [6-7]. Disaster recovery is one way to prevent application downtime. The Disaster Recovery is a term for recovery and the resumption of important technological assets in a disaster. It can include tasks such as continuing individual systems or restoring all important aspects of the Information and Technology (IT) environment [8]. From the understanding of disaster recovery, we can conclude a disaster recovery plan is a plan to recover IT infrastructure from disasters or other threats that are dangerous to information technology infrastructure, the effort to restore IT infrastructure is intended so the information system can run normally again after being threatened, because IT infrastructure is not just tool, but human and technical is also IT Infrastructure [9]. Corresponding to Geoffrey (2006) the benefits provided by disaster recovery include: Provides a sense of security; Minimize the risk of being late; Ensures the reliability of the standby system; Provides standards for testing plans; Minimize decision making when disasters occur [10].

2.3. Business Contunity

Business Continuity is a business aims to make business continue without obstacles. With a good business countinuity plan the organization can respond to possible incidents (that could damage the
resources) in an efficient and effective way. In making a business run without constraints, it must have a plan to enable the business to continue, even natural disasters are not an obstacle. Based on disasterrecovery.org we must do several things for a business to continue, including the Policies and Strategies, Risk Management and Business Continuity Plan [11-12].

2.4. Distributed Replicated Block Device

Distributed Replicated Block Device (DRBD) is a distributed storage system for the GNU / Linux platform consists of kernel modules, some user space application management, and some shell scripts and is usually used on High Availability (HA) clusters [13]. So DRBD makes it possible to duplicate block data on multiple servers or virtual servers. DRBD allows a server to back up automatically so that if there is an interruption on the main server, there are still other backups as shown in Figure 3.

![Figure 3. DRBD Process and Its Illustration](image)

3. Method

According to Cerullo and Michael 2014, the business continuity planning process should address three interdependent objectives there are identified major risks of business interruption, develop a plan to mitigate or reduce the impact of the identified risk also train employees and test the plan to ensure that it is effective. So the implementation first, we have to identify the threat that will occur then develop a new architecture and infrastructure to make ensure it is safe to implement and last we have to test the implementation with some measurements [14]. To make a business sustainable, it must meet two main requirements (policy and strategy, risk management) and another set of business continuity plans. For more clearly the flow of research conducted by Figure 4:

![Figure 4. Research Flow applies Business Continuity Planning](image)
4. Finding and Discussion

4.1. Finding
Disaster Recovery Planning is a backup plan or a return of a gradual and conceptual disaster. Development of Disaster Recovery Planning (DRP) varies according to the conditions are desired for the implementation of mitigation, in creating this DRP focuses on returning data backups in the event of a database disaster and the information system can continue to run as it should. The development of DRP in this study applies the concept of Business Continuity Planning which contains five important components: Identification, Analysis, Design, Execution and Measurement.

4.1.1. Identification. Before making disaster recovery planning, we conducted a data search related to disaster events occurred in Semarang, because the Datacenter of our research object, namely the UNNES comprehensive system and the Online Examination System, was in Semarang, Central Java. To get data with high validity, we use mature data from the Badan Nasional Penanggulangan Bencana / National Disaster Management Agency (BNBP). The following result from data searches related to natural disasters in Semarang.

| Kode | Bencana | Jalur | Cordana | Karhut (Jawa) | Kurang | Cepat | Kerusakan peralatan | Kerusakan (unit) |
|------|---------|-------|---------|-------------|--------|-------|-------------------|-----------------|
| 102  | TANAH LONGSOR | 28 | 2 | 2 | 18 | 7 | 13 | 18 | 0 | 0 | 1 |
| 106  | PUTING BELING | 23 | 6 | 7 | 120 | 7 | 11 | 43 | 0 | 3 | 1 |
| 101  | BANJIR | 8 | 1 | 0 | 14,160 | 0 | 2 | 4 | 146 | 0 | 0 |
| JUMLAH | 39 | 3 | 9 | 14,337 | 14 | 26 | 65 | 146 | 3 | 1 |

*Figure 5. Impact of natural disasters have occurred in Semarang [15]*

4.1.2. Analysis. Based on the data we have got through BNBP data, there are 59 natural disasters in Semarang, and of the 59 disasters that occurred, there were 254 damaged buildings can be seen through Figure 5. The results of the identification show the need for Disaster Recovery Planning.

4.1.3. Design. In making the required disaster recovery topology design, firstly we looked at the initial design of the CBT and UNNES Comprehensive FMIPA System. Seen in Figure 6. if the compressed system is damaged, the synchronizing API will not work and will cause damage, so the researchers propose to redesign by separating the web server and database server so if there is damage to one of them, there will be backups still function can be seen in Figure 7.

*Figure 6. Initial Design of comprehensive and CBT Information Systems.*

*Figure 7. Design of implementing Disaster recovery*

4.1.4. Execution. One method in business process recovery is to restore the backup data itself. Data backup is one important element, the method of data backup has been applied is the disk mirroring...
method, which is making an exact copy of the main data center, data backup done using daily, weekly and monthly backups as well as real-time backups apply the DRBD concept. In this implementation, DRDB is used to mirror Synchronous data so there will be a real-time backup between the two systems.

4.2. Discussion
To ensure a wide range of safe and appropriate conditions, the researchers conducted several kinds of measurements, including backup speed and reliability of backups. By measurement conducted by researchers can confirm the concept of DRBD can back up data automatically and safe to use as a substitute for the primary server in the continuing business processes. The measurement applied in several topologies. This is because the researcher wants to test whether if more backup servers (nodes) are created the backup function can continue to run effectively. For more details can be seen in Figure 8.

![Multi Node Backup Server Testing Topology](image)

**Figure 8. Multi Node Backup Server Testing Topology**

4.2.1. Measurement Of Backup Speed. Backup speed testing is a test to find out how fast the backup process, faster the backup function running in, losing more data can be avoided. Tester does several experiments with the assumption once the experiment adds the same record (data line). Tester adds 10 records to 10 fold experiments with nodes vary from 1 node to 3 nodes. The results of the backup speed test can be seen in Table 1.

| Testing | 1 Node | 2 Node | 3 Node |
|---------|--------|--------|--------|
| 1       | 0.43   | 0.71   | 2.00   |
| 2       | 0.25   | 0.50   | 2.67   |
| 3       | 0.25   | 0.38   | 1.75   |
| 4       | 0.33   | 0.50   | 1.80   |
| 5       | 0.30   | 0.78   | 2.67   |
| 6       | 0.33   | 0.57   | 2.67   |
| 7       | 0.43   | 0.30   | 1.75   |
| 8       | 0.25   | 0.60   | 2.33   |
| 9       | 0.38   | 0.44   | 1.80   |
| 10      | 0.38   | 0.67   | 2.33   |

![Backup Speed Test Results](image)

**Figure 9. Measurement Chart of Backup Speed**

We can see the results of the backup speed test in Figure 10, shows the more nodes can inhibit the speed of data backup. By seeing the inhibition, the researcher made a reduction in the node with the aim the backup can take place effectively.
4.2.2. Measurement of Reliability Testing. Reliability testing is used to see whether the effectiveness of backup process even though the data backed up in the hundreds to millions of records. This test is done by using one node to see the maximum ability of a node in working to back up data. The data entered varies from 100 to 1,000,000, the number of rows of data. Taking up the table we are using is the same and there is no data blob.

| Number Test | 100 record | 1000 record | 10000 record | 100000 record | 1000000 record |
|-------------|-------------|-------------|--------------|---------------|----------------|
| 1           | 1.2         | 4.3         | 8.3          | 11.3          | 15.2           |
| 2           | 0.98        | 4.6         | 7.9          | 10.8          | 14.2           |
| 3           | 0.86        | 4.15        | 8.5          | 11.7          | 15.8           |
| Average     | 1.01        | 4.35        | 8.23         | 11.27         | 15.07          |

The results of tests carried out as shown in Table 2, show the speed continues to slow down with the addition of records. However, the speed is still in seconds can back up millions of data records showing the backup is quite effective.

5. Conclusions

DRBD can be a solution as disaster recovery, especially in backing up data between the main server to the backup server. With DRBD the data backup process can effectively done, seen from the test result. From the results got from testing the backup speed, more backup nodes or points can slow the backup process, so in this study, we applied just one backup so the backup process was carried out more effectively. While the results got from backup reliability testing can be concluded, the backup process is quite effective where the addition of a record number of millions of lines can be reserved in seconds.

References

[1] Alhazmi, O H., and Yashwant K. M 2013 Proc. Annu. Reliab. Maintainab. Symp. (RAMS), IEEE
[2] Budiman, K, Toni P, and Amie P 2018 E3S Web Conf. Vol. 31 (EDP Sciences) p 1.
[3] Bhattacharya S, Roy A, Sen S, & Debnath N C 2017 IEEE Int. Conf. Ind. Technol. (ICIT) p. 1238
[4] Ammar, Moustafa, et al. 2016 8th IFIP int. conf. new technol. Mobil. secuir. (NTMS). IEEE.
[5] Krein, Philip T 2017 "Data center challenges and their power electronics." CPSS Transactions on Power Electronics and Applications 2.1 39-46.
[6] Sahi, A., Lai, D., & Li, Y. 2016 Comput. biol. med. 78 1-8
[7] Routray, R R, et al 2012 Method and system for automated integrated server-network-storage disaster recovery planning. U.S. Patent No. 8,121,966.
[8] Irfansyah B, Saedudin RRD, Rahmat B, 2018, Proceeding Eng. vol 5 1454
[9] Sirkemaa, Seppo. 2015 J. Emerg. Trends Comput. Inf. Sci 6(11) 614
[10] Geoffrey H W 2006 J. J. Dedic. Bus. Contin. 5 10
[11] Torabi, S Ali, Ramin Giahi, and Navid Sahebjamnia. 2016 Saf. sci. 89 201-218
[12] Disaster Recovery Organization 2019 Business Continuity Planning [Available from: https://www.disasterrecovery.org/]
[13] Sugeng P, and Muhammad A F 2017 J. Politek. Caltex Riau 3 (1) 59
[14] Cerullo V, and Michael J C 2004 J. Inf. Syst. Manag. 21(3) 70
[15] Badan Nasional Penanggulangan Bencana 2019 Data Informasi Bencana Indonesia (DIBI) [Available from: http://bnpb.cloud/dibi]