DEVELOPMENT OF BACKUP, REPLICATION AND MONITORING SERVER AS SOLUTIONS DISASTER RECOVERY FOR VIRTUALIZATION SERVER IN THE COMMUNICATION AND INFORMATION OF WEST JAVA PROVINCE

Ferly Adrianus[1], Angga Setiyadi, M.Kom[2]

[1,2] Informatics Engineering - Universitas Komputer Indonesia
Jl. Dipatiukur 112-114 Bandung
E-mail : ferly.pcrg10@gmail.com[1] , angga.setiyadi@email.unikom.ac.id [2]

ABSTRACT

Communication and Informatics Office (DISKOMINFO) is a large government institution and has a large number of employees and a large scope of work, so it has great data to be managed and of course must be well organized. To meet the needs of data management, DISKOMINFO requires a large computing, where the server room is full and has not had a backup server and not yet optimal in the use of the server plus the amount of costs incurred for maintenance of the entire server (maintenance and electricity). DRC server virtualization using HOT type with tools used Vmware ESXi 5.5, Veeam backup & replication version 9 and Network Attached Storage (NAS) with FreeNAS 9.10 operating system, where backup and replication become scenarios in countermeasures. Then to see the server status is built server monitoring program and provide notification when there is server down. Some servers are consolidated into a single physical server and build server backups by replicating servers. Based on test results that have been done, application of DRC server virtualization is very effective. Time of down time only 1-3 seconds so that the information system running stable on the main server condition down. And can also optimize the use of servers and reduce the cost of purchasing or maintaining the server. With replication and restore can make the addition, repair and maintenance server quickly.

Keywords: Virtualization, ESXi, Veeam, Backup and Replication server, Failover, Restore, FreeNAS, Network Attached Storage (NAS), Disaster Management.

1. INTRODUTION

The Office of Communication and Informatics (DISKOMINFO) is an agency responsible for the processing of information within the government environment of West Java Province. Large government agencies and have a large number of employees and a large work scope, so have great data to manage and of course must be well organized. DISKOMINFO currently has a web server, mail server, database server, and server application that has a total of twenty-six servers. Within a period of one to two years DISKOMINFO can procure three new servers to meet the needs of computing. With the addition of the server of course DISKOMINFO must pay a considerable cost and the server room increasingly full year and the cost of electricity continues to increase.

Server will also affect the increase in server room temperature. The air conditioner can fit in a new procurement device to keep the server room temperature cool. Certainly a problem if every new procurement server DISKOMINFO must spend a very large cost and electricity costs continue to increase. Room to put the server full and room temperature will increase if air conditioner is not done addition. Another problem faced by DISKOMINFO is the not yet optimal use of the server, so the addition of new servers is an inefficient step and has not had a disaster recovery center as an attempt to restore information technology services in the event of a disaster. By 2016, DISKOMINFO servers that have once downed are servers that have hostname eoffice.jabarprov.go.id, nms.jabarprov.go.id, intranet.jabarprov.go.id and diperta.jabarprov.go.id with an average Long downtime less than three hours. The down server paralyzes the existing service on DISKOMINFO and waits until the server is up again to perform the service.

To overcome down server and to keep the service running stable, it takes disaster recovery center system, where backup and replication server as scenario of disaster recovery center. Of course, data and information systems that continue to run is very important. DISKOMINFO requires backups if the information service is running is interrupted or an unexpected disaster. Replication is required when the existing system will be made a replica that will be used in another location or applied to the new device that will replace the old device. Replication is also used to create a replica system of the main system as a backup in case of a disaster on the main system. Replication is done so that there is no difference between running system with backup system and system applied to new device with same function with main system.

To overcome this problem, the DISKOMINFO required consolidation of these servers into a physical server using virtualization. There by reducing the amount of physical server usage and build Disaster recovery server virtualization as an effort to cope with disaster.

Based on the problems studied, the purpose of writing this thesis proposal report is to build disaster recovery server virtualization system in DISKOMINFO West Java.

The purpose of this research are:

1. Maintaining the stability of information technology services running on DISKOMINFO.
2. Minimize system down time during disaster.
3. Optimize physical server usage in DISKOMINFO.
4. Minimize the cost of server procurement, electricity used and place the server room.

2. CONTENTS OF RESEARCH

2.1 Backup

In information technology, the workings of backups are to create backup data by copying or archiving computer data so that data can be reused if there is damage or loss. Backup destination to restore data when the data is lost, either because erased or damaged (corrupt) and restore certain point data in the past.[4]

Backups require users to duplicate data, which ultimately depletes storage media capacity. This encourages the discovery of technologies for the storage of backup data, such as deduplication and compression. Factors doing backups are viruses, hard drive damage, natural disaster, loss and other damage due to many causes. [4] So the benefits of backups can use the last data that is backed up when the main data is damaged or lost. This can reduce the loss of things that do not want to happen on important data.

Backup methods are known in the world there are 4, as follows:

1. Full backup :
   Full copy of the computer includes user data and the operating system itself
2. Incremental backup (backup upgrades)
   Copy all data changed since the last time doing a full backup or differential backup. Advantages over a shorter time, Backup faster than full backup, requires a temporary place smaller than that required by full backup. And the lack of time for restore very long.
3. Differential backup
   Same as incremental type but archive bit is not deleted after backup. This is done after a full backup, after a change of data and backup time is not too long.
4. Mirroring (mirror backup)
   Same with full backup, but the data is not compressed or compressed (with .tar, .zip, or others) format. Advantages of the most rapid backup method when compared with other methods for copying data and folders to the destination media without compacting. The drawbacks cause storage media should be large enough. [5]

2.2 Replication

Replication is a technique for copying and distributing data and database objects from one database to another and performing synchronization between databases so that data consistency can be guaranteed. By using this replication technique, data can be distributed to different locations via a local network connection or the internet. Replication is also possible to support the performance of applications, the dissemination of physical data in accordance with their use, such as online transaction processing and DSS (Desiscion Support System) or distributed processing databases through multiple servers. [6]

The benefits of replication depend on the type of replication but in general the replication supports the availability of data every time and wherever necessary.

The other advantages are:

1. Allows multiple locations to store the same data. This is particularly useful when they need the same data or require separate servers in the creation of report applications.
2. Application of online transactions apart from reading applications such as online database analysis process, data smarts or data warehouse.
3. Enabling great autonomy. Users can work by copying data when not connected and then making changes to create a new database when connected
4. Data can be displayed just like viewing the data using a Web-based application.
5. Improve reading performance.
6. Bringing data closer to the location of individual or user groups. This will help reduce the problem due to data modification and query processing performed by many users because the data can be distributed over the network and data can be shared based on the needs of each unit or user.
7. Use of replication as part of a standby server strategy.

Replication can be used if an organization or company is supported by hardware and software applications in a distributed system. Different applications have different requirements for autonomy and data consistency. Replication is required in the diffused system if the conditions are as follows:

1. Copy and distribute data from one or more locations.
2. Distribute the results of copy data based on schedule.
3. Distribute data changes to other servers.
4. Allow multiple users in multiple locations to make changes and then combine modified data.
5. Build data applications using online and offline equipment.
6. Build a Web application so users can view large volumes of data.

Replication Method

1. Snapshot replication

Distributing data can be viewed at any given moment without updating. Usually used when requiring data display such as: price list, catalog, data used for decision making. These data are only 'read only'.

This replication helps when:

a. Data is mostly static and does not change frequently
b. Can receive copies of data that has exceeded the time limit specified.
c. The data is small.

2. Transactional replication

Consistency maintaining of transactions.

3. Merge replication

Merge replication allows users to work and change data according to their authority. If server is not connected to all locations in the topology, the replication changes to the same data value. [6]

2.3 Differences between Backup with Replication

Differences between backups with replication, by definition, backup outlines involve making copies or copies of data. Replication is the act of copying and then moving data between sites of the company. This is usually measured in Recovery Time Objective (RTO) or the required recovery time and Recovery Point Objective (RPO) or acceptable data loss tolerance. Required backup requires a tape library (usually VTL does disk-to-disk backup) and some places to store archival tapes or other storage media. While the need for replication is an identical infrastructure, so as to require additional costs to provide identical infrastructure.[7]

Backups focus on compliance and detailed recovery, such as restoring a single user's email from 5 years ago. Backups are usually used for everything in the company, from critical production servers to desktops. Backups usually depend on snapshots which are copies of the data set taken at a predetermined point. Relatively inexpensive way to avoid data loss. It just does not guarantee continuity of operation.

Replication focuses on restoring business continuity of quick and easy return of operations after a disaster or system malfunction. Minimizing the goal of recovery time (RTO) is the main point of replication. Replication is often used for mission-critical applications that must always be active and running. Focused on ensuring business and process applications are always available, even after a disaster. Obviously the cost for expensive replication setups, the need for infrastructure readiness and maintenance costs. [7]

2.4 Disaster Recovery Center (DRC)

Disaster Recovery Center is the ability of infrastructure to re-conduct operations as soon as possible in the event of significant disruptions such as unforeseen catastrophes. An example of this is when the catastrophes of some of the world's major companies headquartered in Word Trade Center can still operate (soon recovering their operations soon), as they have prepared a number of DRCs to anticipate the unwanted disaster.

In general, DRC serves to:

1. Minimize financial and nonfinancial losses in the face of natural disasters in the form of physical and important data information for the company.
2. Enhance the sense of security in business relationships among personnel, suppliers, investors, and customers.

Infrastructure disaster recovery includes data center facilities, wide area network (WAN) or telecommunications, local area network (LAN), hardware, and applications. From each of these sections must determine the most appropriate disaster recovery strategy in order to provide an effective and appropriate solution to the needs of the company.[9]

In accordance with Indonesian regulations that DRC locations have a minimum distance of> 40 km from the Data Center center and are outside the disaster mitigation radius (Volcano, Tsunami, Flood, etc.). Our DRC location is also not on the geological fault line, Low Becana Risk Induction in Indonesia, network access is adequate and accessible.

Type DRC

1. Cold DRC

Cold DRC provides the same system as the data center location where applications and data will be uploaded before the DRC facility can be used, but the process of moving from the data center to the DRC location will be done manually.

2. Warm DRC

Warm DRC will provide computers with all its components, applications, communication links, and data backups are the most updated, where the system does not automatically move but there is still a manual process although done to a minimum.

3. Hot DRC

Hot DRC is set up as soon as possible business operations, systems with applications, the same communication link has been installed and is available in DRC locations. Data continues in the backup using a direct connection between the data center and DRC location, and business operations will run on the spot without having to shut down the system in the old data center. [9]

2.5 Vmware vSphere / ESXi

VMWare vSphere is a virtualization platform that is used as a virtualization platform for a variety of tools, especially those associated with server tools. Virtualization here means that a physical device, which can be seen as a form of a PC or associated with it, can be broken down into multiple virtual devices that each stand alone and have their own functionality. Of course not all PC devices can be given this kind of treatment. Only special tools such as servers can do this kind of thing, with good results. The logo of VmWare vSphere can be seen in Figure 2.2 as follows.

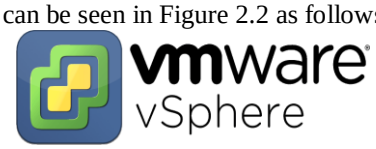


Figure 2. 2 Vmware vSphere Logo.

Vmware ESXi is used to encapsulate virtual machines where there are disk configurations, files and others that make up a physical configuration of a whole hardware. ESXi can be likened to an operating system that underlies the formation of a virtual machine.[11]

2.6 Veeam Backup and Recovery

Veeam Backup & Replication is built specifically for the corporate virtual environment. This software was created specifically to perform the backup and recovery virtual machines (VM), regardless of what virtual platform to use, the operating system, or the type of storage (storage). The veeam logo can be seen in Figure 2.3 as follows.



Figure 2.3 Aplication Veeam Backup and Replication Logo.

With a single license and integrated console, this app can protect all virtual infrastructure with industry-standard functions. Example is Instant VM Recovery, granular files and application recovery, near -continous data protection (near CDP), and much more.

Regardless of using VMware, Hyper ± V, or a combination of both, Veeam already supports the latest hypervisor release: VMware vSphere 5.1 and Windows Server 2012 HyperV..[13]

2.7 Problem Analysis

In analyzing problem of server systems running in DISKOMINFO West Java, conducted interviews and direct observations to related employees and server rooms. Based on the results of problem analysis conducted, it can be concluded some problems on the server system in DISKOMINFO West Java, namely:

1. DISKOMINFO has no disaster recovery in information technology infrastructure in dealing with disaster in DISKOMINFO. So when the information technology infrastructure gets a disaster then the existing service can't work.
2. How to implement disaster recovery on virtualization technology with backup, replication in DISKOMINFO. This step is taken for Perform server consolidation, by implementing server virtualization can save the number of servers used physically. By doing backups and replication provide ease in tackling disasters and in addition of the same system.
3. Not maximum usage of servers owned by DISKOMINFO. Of all the existing servers, the use of the server has not been optimal, judging from the percentage of memory usage and the processor is still below 40%. Only a few servers reach above the 40% percentage like the application server at any given time.
4. Costs magnitude incurred DISKOMINFO for the procurement of servers and supporting infrastructure in each year. Within one year DISKOMINFO can do server addition of three unit server. Of course for the procurement of three units of servers incur large costs and also the addition of electricity costs.

2.8 DISKOMINFO Network Topology Analysis

The network topology available on DISKOMINFO now is as in Figure 2.4. The servers contained in DISKOMINFO are accessed by government agencies located in West Java such as RSUD, KEMENDAGRI, OPD, UPTD and also from international links. Client will connect to DISKOMINFO server through core switch, DISKOMINFO DNS server and firewall. Of course the server also has a public service that will be accessible by the general public.

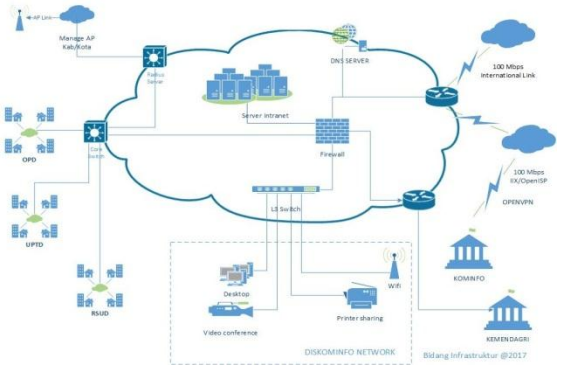


Figure 2.4 DISKOMINFO *Network Logic Topology*.

The servers contained on DISKOMINFO can be accessed from various places. In Figure 3.3 there are twenty-six servers in DISKOMINFO accessed by many government agencies such as KEMENDAGRI, DISKOMINFO branch, RSUD, UPTD, OPD and Manage AP Kab / Kota and international links. Desktop, wifi and video conferencing available on DISKOMINFO can access the server by passing core switches and firewalls.

2.9 DISKOMINFO Server Network Topology Analysis

In Figure 2.5 is the server network topology currently available in DISKOMINFO. There are twenty-six server detail servers. In this server network topology there is no backup server. So when a disaster occurs it can cause DISKOMINFO service to be interrupted and stopped until the server is repaired.

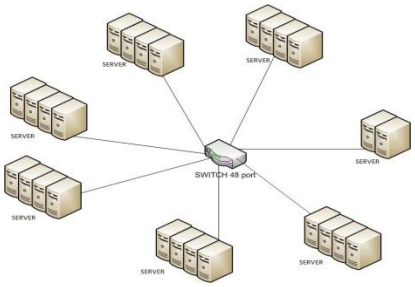


Figure 2.5 DISKOMINFO Server Network Topology.

The topology used in the DISKOMINFO server network is a star topology. Be able to communicate each other server using only one path.

2.10 Network Topology Be Built

The following is the design of the server virtualization network topology to be built, can be seen in Figure 2.6. By maintaining the existing network infrastructure, the server device used only five servers, where the other servers are consolidated into a single physical server using virtualization technology. In a physical server there are five to six servers consolidated. The number of servers that can be consolidated in a single physical server depends on the server's physical specifications and the server load.

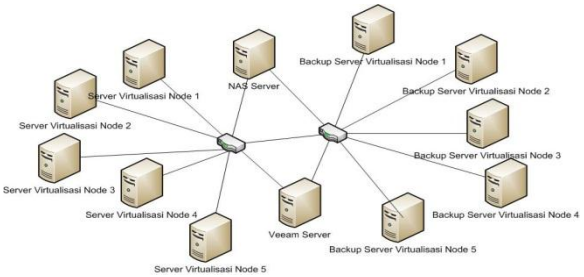


Figure 2.6 Proposed Server Network Topology.

Topology in use still used star topology. Five servers are used as main server virtualization and five other servers as server virtualization backups. One server as a NAS server for data storage media backup server virtualisation and one server as a server in charge of managing the backup, replication, failover and monitoring server. So the number of servers used is twelve server units. The number of servers used is reduced from twenty-six servers and saves as many servers as fourteen servers. The other fourteen servers can be used for other needs.

2.11 Backup Test Server Virtualization

In testing the backup is done by two methods namely full backup and incremental backup. Observations of these tests were performed three times at different times and days, in which the VM size was 100 GB. The result of backup testing with full backup method can be seen in table 2.1 below.

Table 2.1 Full Backup Testing.

Testing to-	Test time	Duration	Throughput (All time) MB/s	Status
1	20:00 WIB	0:22:30	11.0	Succsess
2	12:05 WIB	0:29:49	8.1	Succsess
3	21:00 WIB	0:30:39	7.8	Succsess

Testing to-	Time (WIB)	Down Time		Testing status
		Main to secondary server (secon)	Secondary to main server (secon)	
1	21:00	1	7	Succsess
2	20:24	1	4	Succsess
3	19:37	2	3	Succsess

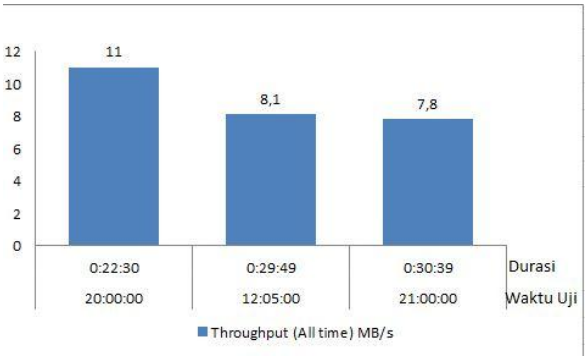


Figure 2.7 Full Backup statistic's testing.

Based on the results of tests that have been done, it appears that the greater throughput then the duration of the backup faster. Full backup can be completed with an average duration of 27 minutes.

2.12 Server Virtualization Replication Test

Replication testing done with two methods of full replication and incremental replication. Observations of these tests were performed three times at different times and days, in which the VM size was 100 GB. The result of replication testing with full replication method can be seen in table 2.2 below.

Table 2.2 Full Replication Testing.

Testing to-	Test time	Durasi	Throughput (All time) MB/s	Status
1	21:00 WIB	0:32:23	7.6	Success
2	16:31 WIB	0:50:34	5.8	Success
3	20:00 WIB	0:46:06	5	Success

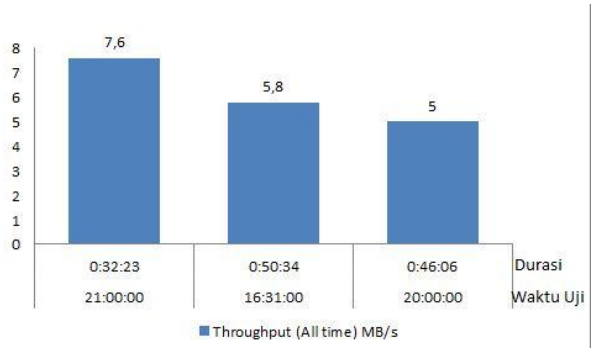


Figure 2.8 Full Replication Statistic.

It can be concluded the duration of rat-rata in doing full replication 43 minutes. The longer duration of time compared to the full backup where it has a difference of average duration of 16 minutes.

2.13 Failover Server Virtualization Testing

Failover testing is done three times, where for this test is done down time observation when main server down to the take over by secondary server and down time when moving from secondary server to main server when it is up again. The results of observations that have been done can be seen in table 2.3 below.

Tabel 2.3 Failover Testing.

Testing to	Time (WIB)	Down Time		Testing status
		Main to secondary server (secon)	Secondary to main server (secon)	
1	21:00	1	7	Success
2	20:24	1	4	Success
3	19:37	2	3	Success

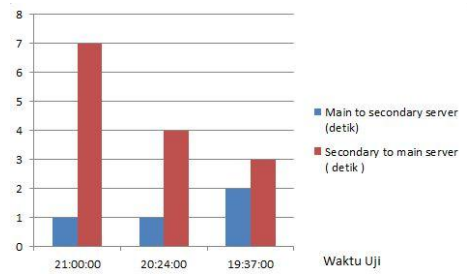


Figure 2.9 Failover Testing Statistics.

In the failover test, the average down time when the main server is down and the take over secondary server is 1.3 seconds. When the switch back from secondary to the main server is 4.6 seconds.

2.14 Testing Server Virtualization Restore

The VM restore test is performed three times, where testing is performed on different days and days with the same VM. The results of the test restore can be seen in table 2.4 below.

Table 2.4 Restore Testing.

Testing to-	Test time	Durasi	Throughput (All time) MB/s	Status
1	6:49	0:29:52	5	Success
2	20:16	0:23:32	7	Success
3	23:57	0:26:29	6	Success



Figure 2.10 Restore Testing Statistics.

In the restore test, from a different time obtained a restorative duration of 26 minutes with an

average throughput of 6 MB / s where the amount of data full restor 100 GB VM

2.15 Server Virtualization Monitoring Tests

The software is built for monitoring web-based servers. So that required testing of software. Software testing is a step to find errors and deficiencies in software built so it can be known whether the software has met the criteria in accordance with the purpose or not. The test method used in this software is the Black box testing method. Black box testing focuses on the functional requirements of the software. Black box testing method consists of two stages of testing, namely alpha testing stage and beta testing stage.

Based on the results of testing done it can be concluded that the monitoring server built is running in accordance with the expected both in terms of validation and error handling process. The conclusions obtained from the interviews in the beta testing phase, that the current research is needed DISKOMINFO, by applying virtualization one physical server can handle multiple application servers running on DISKOMINFO later. Optimization of server usage can be achieved, easy to perform maintenance and replacement server and efficiency of resources both in terms of electricity usage and server can be physically suppressed or minimized. Monitoring the built server provides easy monitoring of server status and easy to use.

3. CONCLUSION

From the results of analysis and implementation carried out, can be drawn some conclusions are:

1. The design of disaster management system with backup, replication and failover solution on server virtualization is successful. System backup files can be restored and replace damaged system files, and server replication results performed exactly the same as the main server. In testing the system is able to obtain time downtime with a value of 1-3 seconds during the process of failover from the main to the secondary server..
2. The design of disaster management system on server virtualization technology is able to maintain the stability of information technology services running on DISKOMINFO when main server down.
3. With the implementation of server virtualization technology, the use of physical servers can be optimized.
4. Costs incurred for information technology needs can be minimized.

Realizing that the completion of this final project is still far from perfect, for it is expected to be a material or one reference for other readers in order to create disaster management system on server virtualization better. Some suggestions that can be done for the development of this final task, among others:

1. Adding ESXi server nodes and for managing ESXi nodes can use Vmware Vcenter.
2. Add a mirror server NAS for data recovery in case of a disaster on NAS.
3. Can apply VMFS volume or Fiber channel and NFS in add datastore ESXi server.
4. Can use other tools during backup and replication scenarios on server virtualization such as NAKIVO backup and replication.

REFERENCE

[1] Novi. (2015, Mei) prezi.com. [Online]. https://prezi.com/4ewtum1s9xjp/logo-adalah-suatu-identitas-yang-dipergunakan-untuk-menggamb/

[2] Sartika Wulandari. id.scribd.com. [Online]. https://id.scribd.com/doc/220441465/Visi

[3] Handoko Reksohadiprodjo, "Struktur Organisasi," p. 74, 1992.

[4] Tiwo Satriatama, "Pengertian, Tujuan, Fungsi, Kriteria dan Pentingnya Backup Data ," November 2015.

[5] Dony Donker. scribd. [Online]. https://id.scribd.com/document/28184829/Kinerja-Windows

[6] TSI Perbankan. elearning.gunadarma.ac.id. [Online].learning.gunadarma.ac.id/docmodul/AS400/./04Replikasirev.pdf

[7] Chris Mellor. (2012, february) Zerto. [Online]. http://www.zerto.com/blog/replication/backup-and-replication-what-is-the-difference/

[8] Muhammad Dzulkarnaen, "Implementasi Layanan Jaringan," Telkom University, Bandung, April 2016.

[9] Nugroho P Yudho, Robby Hasan P Farid Ridho, "Disaster Recovery Center and Disaster Recovery Plan ," November 2012.

[10] Adian Fatchur Rochim, Kodrat Iman Satoto Krisnawan Hartanto, "Implementasi Virtual Private Server Menggunakan Xen Hypervisor," Universitas Diponegoro, Semarang, 2011.

[11] Ibnu Febry Kurniawan Rachmad Aziz, "Implementasi Teknologi Awan untuk Layanan Infrastruktur," Universitas Negeri Surabaya, Surabaya, 2016.

[12] Gilby Benaya Lesar, "PERANCANGAN DAN PEMBANGUNAN NETWORK ATTACHED STORAGE UNTUK DATA CENTER AKADEMIK SEKOLAH DASAR," Universitas Komputer Indonesia, Maret 2015.

[13] PT.mandawanimandiri. mandawani.com. [Online]. http://www.mandawani.com/id/solusi/backup-recovery.html
[14] Ahmad Paudji Hendra Suputra, "Perancangan dan Implementasi Jaringan Small Office Home Office Berbasis Network Attached Storage," Universitas Komputer Indonesia, Bandung, 2015.
[15] Melwin Syafrizal, Pengantar Jaringan Komputer, Dwi Prabantini, Ed. Yogyakarta: Penerbit Andi, 2005.
[16] Mulia Rizqina, "Bandwitd Monitor," Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, 2012.
[17] Afwan Bahtiar, "Monitoring Jaringan dengan PRTG Traffic Grapher," Universitas Diponegoro, Semarang, 2009.
[18] Ceppy Efraim, Sandy Hermawan Sidik Nurcahyo, "Pembangunan Website di CV.Surya Mitra Buana," Universitas Komputer Indonesia, Bandung, 2016