Clustering Storage Method for Digital Evidence Storage Using Software Defined Storage

Mohammad Faruq Afif¹, Mukhammad Andri Setiawan², Yudi Prayudi³
Department of Informatics, Faculty of Industrial Technology, Universitas Islam Indonesia, Yogyakarta. INDONESIA
14917149@students.ui.ac.id, andri@uii.ac.id, yudi.prayudi@uii.ac.id

Abstract. The increasing of cybercrime means an increase in the number of digital evidences produced in these criminal activities. Also, to pay attention to the security and integrity of digital data, the construction of digital evidence storage must pay attention to the need for convenience in adding storage and the need for investigators to avoid geographical problems in carrying out their duties. An ideal implementation of the problem is the development of network-based digital evidence storage using the Software-Defined Storage to build a clustered storage system. In this study, we build a clustered storage system using Ceph that will be functioned as digital evidence storage. Ceph is a Software-Defined Storage which is designed to provide excellent performance, reliability and scalability. On the other hand, since digital evidence is fragile, then the security of storage system must also be considered so that the stored digital evidence in the storage system can be accepted in court. The security includes aspects of confidentiality, integrity and availability aspects. We were able to build a storage system using Ceph and as a result, our system storage has met the aforementioned scalability, confidentiality, integrity and availability aspects. The storage system is expected to contribute in terms of digital evidence storage and preservations.

Keywords. digital evidence, evidence storage, clustered storage, software defined storage, ceph

1. Introduction
Cybercrime is a term that refers to criminal activity with computers or networks. The computer becomes a tool, target or place of crime. Like other criminal activities, cybercrime will certainly leave a trail/evidence that can be used for investigation. Evidence in cybercrime cases can be in the form of physical evidence or digital evidence. Physical evidence will be stored in the evidence storage room while digital evidence will be stored in evidence storage. Considering that cybercrime activities are increasing, so that evidence quantity in these activities is also increasing. As the quantity of digital evidence increases, the quality of digital evidence that is getting better also requires more space in storage time by time.

Therefore, digital evidence storage must be secure, adequate, dedicated to large storage solutions and have excellent scalability. Digital evidence storage must also be able to work automatically, thereby
reducing the obligation of the examiner or investigator in carrying out administrative tasks related to the system. Furthermore, digital evidence storage must accommodate the needs of examiners and investigators who may be geographically separated to be able to carry out their duties in digital forensic investigations and the needs of examiners or investigators for easy access to digital evidence so that if necessary digital evidence can be examined in another place to know the further investigations. An ideal implementation of the problem is a centralized evidence storage that allows evidence to be accessed securely from a remote location. This is possible by the development of network-based digital evidence storage.

Some research on the development of network-based digital evidence storage has been carried out by several researchers such as Davis et al. [1] who designed a digital evidence custodian (DEC) architecture using Network Attached Storage (NAS) and Storage Area Networks (SAN), and Ali et al. [2] who created a Chain of Custody Reflex system based on SAN and web-based technology as network-based centralized storage architecture[2]. However, these researches has not yet discussed the need for ease of additional storage while we knew that the weakness of using SAN and NAS technology is limited scalability.

On the other hand, there are currently many studies on storage systems that use software-defined storage (SDS) instead of traditional storage technologies such as SAN and NAS. SDS offers better things in terms of cost, agility, scalability, reliability, and multi-tenancy. In terms of scalability, traditional storage can only be scaled up to a maximum of 4 - 8 controllers, while SDS can scale up to hundreds of thousands of nodes - meaning theoretically it can be scaled indefinitely [3]. Therefore, the use of SDS to replace SAN and NAS in the development of digital evidence storage systems can be another solution that can accommodate the need for convenience in adding storage. One of the SDS that is widely discussed in research on its excellent scalability is Ceph. Gudu [4] has proven the capability of Ceph scalability by adding Object Storage Daemon (OSD) on a system running up to 20 OSDs (10 nodes). Based on the research conducted, Ceph's performance increases steadily with the number of OSDs.

According to some of the advantages of Ceph as SDS compared to traditional storage such as NAS and SAN as expressed in previous studies, the authors intend to build digital evidence storage using Software-Defined Storage Ceph as an alternative in the development of network-based digital evidence storage. Considering digital evidence is fragile, then the security of the storage system must also be considered so that the stored digital evidence in the storage system can be accepted in court. The security of a storage system includes aspects of confidentiality, integrity and availability aspects. The storage system is expected to meet the criteria of scalability, confidentiality, integrity and availability aspects.

2. Literature Review

2.1. Digital Evidence

Digital evidence is information stored or distributed on a computer or in digital form that can be used as evidence in court. This information can be in the form of text, images, audio, video that can be found on a computer hard drive, cellphone or smartphone, CD / DVD, flash/memory card and others.

Kuntze [5] defined five rules of evidence for evidence to be considered useful. Evidence must be admissible, authentic, complete, reliable and believable. After digital evidence obtained from crime scene, officer have to immediately make a complete bitstream image of the media on which the evidence is stored. The original should then be stored in a safe place where its integrity can be maintained, while the copy will be examined [6]. Both are stored in a digital evidence storage area in the Forensic Laboratory. Digital evidence storage is an important infrastructure that supports the process of storing digital evidence. To make the criteria for evidence to be received at court, a digital evidence storage system must make information security criteria in the form of Confidentiality, Integrity, and Availability.

2.2. Storage Cluster

Storage cluster is a network of multiple storage systems that behave as one system that works together to improve system performance, capacity, and reliability. In the most abstract sense, a storage cluster consists of several storage servers that can be accessed through a network, usually by installing it as a
virtual filesystem on the server. Features usually include a high level of redundancy and availability. For example, if one server in the storage cluster fails, data can still be accessed from other servers in the cluster. In addition to data availability and ease of access, another benefit to being achieved from using a storage cluster is the ease of adding capacity. Storage cluster can be achieved by using software-defined storage.

2.3. Software Defined Storage

Software-defined storage (SDS) is a term for computer data storage software that enables the management of data storage that is created and managed regardless of the attachment to the underlying hardware. Software-defined storage usually includes a form of storage virtualization to separate storage hardware from the software that manages it. This software provides management policies for a variety of feature options, such as data deduplication, replication, thin provisioning, snapshots, and backups.

One of the open-source defined storage software is Ceph. Ceph is claimed to have the ability to transform IT infrastructure and enable users to manage large data. Ceph was built with RADOS (Reliable Autonomic Distributed Object Storage) as its core. RADOS in Ceph provides a storage system for objects, blocks, and files in a cluster. RADOS makes Ceph flexible, reliable and easy to manage [7]. It allows Ceph to be self-healed and self-manage. In the event of a disaster, Ceph can provide reliability for multiple failures. Ceph detects and corrects failures in each failure zone as disks, nodes, networks, racks, data center lines, data centers, and even various geographic locations. Ceph tries to manage the situation automatically and resolve it as much as possible without data interruption [8].

Another thing that makes Ceph superior is the CRUSH (Controlled Replication Under Scalable Hashing) algorithm. CRUSH is a pseudo-random data distribution algorithm that efficiently and powerfully distributes replicas of objects across heterogeneous and structured storage clusters. CRUSH is designed to facilitate the addition and removal of storage by minimizing data transfer between OSDs. This algorithm accommodates various types of data replication and mechanisms to maintain reliability and distribute data according to user needs [9]. These features make CRUSH suitable for managing the distribution of objects in very large (multi-petabyte) storage systems where scalability, performance, and reliability are very important. CRUSH ensures that data is distributed to all cluster members and all cluster nodes can provide data without bottlenecks.

With RADOS and CRUSH as the basis for its development, Ceph uniquely sends objects, blocks, and file storage in one integrated system. With this, the Ceph storage cluster can accommodate many nodes, which communicate with each other to replicate and redistribute data dynamically.

In general, Ceph storage cluster consists of two types of daemons: Ceph OSD Daemon (OSD) stores data as objects on storage nodes; and Ceph Monitor (MON) keeps a master copy of the cluster map. Ceph storage clusters can contain thousands of storage nodes. The system has at least one Ceph Monitor and two Ceph OSD Daemons for data replication.

3. Research Methodology

3.1. Design

Digital evidence storage is built in a virtual machine (VM) environment. Although built in a virtual environment, this condition can already represent the real condition. The following is a list of hardware and software used in this study:

Hardware: a set of servers with CPU (s) 32 x Intel (R) Xeon (R) CPU specifications E5-2670 0 @ 2.60GHz (2 Socket) 368Gb Memory and 1.6 Tb Hard Drive
Software: Proxmox VE 5.3-8 operating system, Ubuntu 18.04 LTS operating system, Open VPN Server, OpenVPN Client, Ceph Mimic Stable Version 13.2.5, ownCloud Server, ownCloud Client, Wireshark Network Protocol Analyzer.
The system storage design which is built in this study is illustrated in Figure 1.

The digital evidence storage system design consisted of 8 storage server nodes, 2 Ceph monitors (MONs) servers, and 1 Ceph client. Each storage server node has 2 OSDs which will be combined into a storage cluster. Each OSDs has a capacity of 20GBs. Then the Ceph storage cluster will be linked from the Ceph monitor server to the Ceph client. Ceph client acts as a server that will be accessed by investigators using encrypted networks openVPN. In this study, two connection lines were built to access the system, namely through a wired network and wireless network (wireless or GSM). System testing will be conducted on a wireless network using a GSM network to illustrate the situation if the Digital Forensic Laboratory in an area not yet reached by a cable network (Fiber Optic). OpenVPN configuration is also used to secure data transmission. OpenVPN server installed on a virtual machine.

This concept is supported by ownCloud software as a service management and synchronization of digital evidence files between the acquisition file and Ceph client. OwnCloud can manage cloud storage services ranging from users, user groups, limited access, user size quota, automatic synchronization feature, transfer data using SSL encryption and verify checksum for uploaded or downloaded files. OwnCloud Desktop Sync is used to synchronize digital evidence files.

Wireshark Network Protocol Analyzer software is used to test data security. Wireshark is a visual network analyzer and capturing packet tool with facilities that are complete enough to see the data path and protocol used.

3.2. System Testing

At this stage, 4 test scenarios are performed to get the data to be analyzed. The results of tests carried out besides expected to provide good results from scalability criteria, are also expected to meet the criteria of confidentiality, integrity, and availability. These four criteria are very important for the development of evidence storage. Scalability criteria must be met considering that evidence grows exponentially, so evidence storage must be easy to scale. While the criteria of confidentiality, integrity, and availability
must be fulfilled so that evidence meets the five rules of evidence, namely evidence must be permissible, authentic, complete, reliable and believable in order to be accepted and used as evidence at court.

Confidentiality criteria which means safeguarding information from people who are not entitled to access, in this study is conducted by:
- The use of openVPN technology
- The use of https protocol
- User / password authorization with a token

Integrity criteria which means maintaining consistency, accuracy, and trust in data from time to time. Maintaining integrity also means ensuring that data is irreversible. In this study carried out by:
- Applying strong encryption to data storage and transmission media.
- Applying strong authentication and validation on every file access/account login/action that is applied.
- Authentication and validation are done to ensure the legality of access.
- Applying strict access control to the system, i.e. every existing account must be restricted in terms of access rights. For example, not all investigators have the right to access evidence that is actively being examined, only those charged with investigating can access it, while other investigators can only see it.

The purpose of availability is to ensure that the available resources are ready to be accessed at any time by the user/application/system that needs them. In this study, the availability aspect is achieved through the use of Ceph which has the ability of self-healed, self-managed, and reliable against multiple failures.

4. Result

4.1. Scalability Testing

Testing is run by adding 2 nodes into the system which originally had 8 nodes so that there are a total of 10 nodes running in the system. Figures 2 and 3 show the state of the system before and after the addition of new nodes. The total disk capacity before adding nodes is 320GB after adding 2 Nodes with 4 OSDs, the total disk capacity being 400GB. Figure 4 show details of each OSD after adding new nodes. As shown in Figure 4, there are 20 OSD with a capacity of 20GB each, and a total capacity of 400GB. Each OSD (including additional OSD) has a used space of 4.0 - 4.9 GB so that the total used space is 90 GB. When additional OSDs enters the system, Ceph will automatically replicate the data into the additional OSD.

The process of adding these nodes runs smoothly without any system disruption. The easy process of increasing storage can occur because Ceph was developed with a scale-out design. The scale-out design focuses on adding all-new nodes, including disk, CPU, and memory to the existing system. In this type of design, the system will not end with limited storage, but rather, it will benefit from the performance and robustness of the system when adding new nodes so that when there are new nodes added, Ceph's performance also increases.

```
prodep@mon-ceph1:~$ sudo ceph df
[sudo] password for prodep:
GLOBAL:
        SIZE       AVAIL      RAW USED    %RAW USED
... 320 GB  251 GB    69 GB  21.44

prodep@mon-ceph1:~$ sudo ceph df
[sudo] password for prodep:
GLOBAL:
        SIZE       AVAIL      RAW USED    %RAW USED
 400 GB  313 GB    69 GB  21.44
```

**Figure 2.** The system state before adding new nodes

**Figure 3.** The system state after adding new nodes
Figure 4. Details of each OSD after adding new nodes

Figure 5. Results of sniffing files using Wireshark shows that the OpenVPN connection has been encrypted.

4.2. Data Transmission Security Testing

Testing is run by using the sniffing method (tapping) on every packet that passes through the network, then see and analyze the results. The tool used to conduct this test is Wireshark Network Protocol Analyzer.

The test results shown in Fig 5 show random data from the sniffing results. This shows that the openVPN connection and the use of the https protocol in this study make encrypted data transmission, which means that the confidentiality criteria in the system have been met.

4.3. Testing file synchronization

The next test scenario is testing file synchronization using Telkomsel's 4G network in several connection quality parameters with ping time, jitter, bandwidth, and packet loss. Telkomsel's GSM 4G network was chosen because based on the Cellular Network Experience Report in Indonesia in July 2019 released by opensignal.com Telkomsel has the highest value with an average download speed of 12.8Mbps and upload speed of 3.7Mbps [10].
Table 1. Result Of Synchronization Testing File

| No | Connection Type | ping time (ms) | Jitter (ms) | Bandwidth Transmit (Mbps) | Bandwidth Received (Mbps) | Packet Loss (%) | MD5 Source | MD5 Server | Note |
|----|----------------|----------------|-------------|---------------------------|---------------------------|-----------------|------------|------------|------|
| 1  | 4G             | 55             | 169         | 74                        | 5.752                     | 5.45            | 5.29       | 0          | 44847d4eb5a0d 152cf65f533fe2 3ad74 | ok    |
| 2  | 4G             | 45             | 122         | 64                        | 12.427                    | 3.04            | 2.88       | 0          | 44847d4eb5a0d 152cf65f533fe2 3ad74 | ok    |
| 3  | 4G             | 48             | 91          | 63                        | 8.101                     | 1.89            | 1.74       | 0          | 44847d4eb5a0d 152cf65f533fe2 3ad74 | ok    |
| 4  | 4G             | 47             | 100         | 59                        | 21.246                    | 1.05            | 0.905      | 0          | 44847d4eb5a0d 152cf65f533fe2 3ad74 | ok    |
| 5  | 4G             | 39             | 138         | 65                        | 15.582                    | 0.629           | 0.434      | 0          | 44847d4eb5a0d 152cf65f533fe2 3ad74 | ok    |

The file used in this study is a CCTV recording file with the extension .mp4, which is 91MB in size. Testing uses the ownCloud Desktop Client tools so that digital evidence files are automatically synchronized to the server. The research method used is to change the bandwidth with the parameters ping time, jitter and packet loss. Data is taken by comparing the results of MD5 source file hashing and files that have been uploaded on the server.

The test results shown in Table 1 show that using network conditions where the received speed is 0.434 Mbps and the transmit speed is 0.629 Mbps, the results of checking MD5 source files and files that have been uploaded on the server are the same. In other words, file transfers with low bandwidth or poor network quality do not affect file integrity.

This testing scenario is carried out to illustrate that even when synchronizing digital evidence acquisition results with unfavorable network conditions can still ensure the integrity of the acquired digital evidence.

4.4. Test of disconnected nodes

One of the testing scenarios runs is to make the condition of one of the Ceph nodes disconnected when a file transfer is performed. The file transferred in this case is a CCTV recording file with a .mp4 extension measuring 91MB. We make 2 states of the disconnected node ie when 2 nodes are disconnected, and 4 nodes are disconnected then compare the results.

When 2 nodes are disconnected, file transfer from client to server continues to run normally. Fig 6 shows the condition of 2 nodes or 4 OSD down, cluster status is declared healthy. It shows that the disconnected of 2 nodes are minor failure for Ceph. After 2 broken nodes are reconnected, the system will synchronize files. MD5 hashing checking of source files and file servers give no change.

When 4 nodes are disconnected, file transfer from client to server stops. As can be seen in Fig 7, Ceph will do the blocking into the storage system so that the file is retained until only 3 nodes are cut off. When the number of broken nodes is only 3, file transfers can resume normally. And when the system is fully reconnected and declared healthy, the system will synchronize. Checking MD5 hashing of source files and file servers give no change.
Figure 6. Testing With The Condition Of 2 Nodes Or 4 OSD Down, Healthy Cluster Status

Figure 7. Testing with the condition of 4 nodes or 8 OSD down, Ceph did blocking

The system repair process runs automatically. This can occur because the RADOS feature of Ceph allows Ceph to be self-healed and self-manage. RADOS also makes the system flexible, reliable and easy to manage. In the event of a disaster, Ceph can provide reliability for multiple failures. Ceph detects and corrects failures in each failure zone as disks, nodes, networks, racks, data center lines, data centers, and even various geographical locations. Ceph tries to manage the situation automatically and resolve it as much as possible without data trouble [8].

Based on that simple test, it can be concluded that the storage system that is built meets the aspect of availability that is ready to be accessed anytime by the user / application / system that needs it. The results of checking MD5 hashing of the same source file and file server in this test also confirm that this storage system has met the integrity aspect.

5. Conclusion

Based on the analysis, implementation of the storage system and testing that has been done before, it can be concluded that the digital evidence storage can be built using clustering storage method by software defined storage i.e. Ceph. This digital evidence storage is a network-based centralized repository that can be accessed securely from a remote location.

The advantage of using this method is the excellent scalability capabilities that have been proven from previous tests. As a digital evidence storage, this storage system has also fulfilled security aspects, namely in terms of confidentiality, integrity, and availability. So that digital evidence stored in this digital evidence storage system can be for use as evidence in court room.

This research has not focused on the digital evidence’s Chain of Custody (CoC) and preservation yet. Further research is needed regarding the management of digital evidence stored in the system that has been built in this study.

References

[1] Davis, M., Manes, G., & Shenoi, S. (2005). A Network-Based Architecture for Storing Digital Evidence. The International Federation for Information Processing, vol. CXCIV, no. -, pp. 33-42, 2005.

[2] Ali, M., Prayudi, Y., & Sugiantoro, B. (2019). Storage Area Network Architecture to support the Flexibility of Digital Evidence Storage. International Journal of Computer Applications, 182(41), 30–35. https://doi.org/10.5120/ijca2019918496
[3] Paul Chinnaraju, S., Gunasekaran, G., Kumar, N., & Anandan, R. (2018). Transformation from legacy storage to software defined storage—a review. International Journal of Engineering & Technology, 7(2.21), 306. https://doi.org/10.14419/ijet.v7i2.21.12387

[4] Gudu, D., Hardt, M., & Streit, A. (2014). Evaluating the Performance and Scalability of the Ceph Distributed Storage System. 2014 IEEE International Conference on Big Data, 177-182.

[5] Kuntze, N., Rudolph, C., Richter, J. (2010). Securing Digital Evidence. 5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010, 119-130

[6] Shinder, L., & Cross, M. (2008). Chapter 15 - Collecting and Preserving Digital Evidence. In L. Shinder & M. Cross (Eds.), Scene of the Cybercrime (Second Edition) (pp. 623–652). https://doi.org/https://doi.org/10.1016/B978-1-59749-276-8.00015-7

[7] Weil, S. A., Brandt, S., Miller, E., Long, D., & Maltzahn, C. (2006). Ceph: A Scalable, High-Performance Distributed File System. In OSDI.

[8] Singh, K. (2015). Learning Ceph. Birmingham: Packt Publishing Ltd.

[9] Weil, S., Brandt, S., Miller, E., & Maltzahn, C. (2007). CRUSH: Controlled, Scalable, Decentralized Placement of Replicated Data. (November), 31–31. https://doi.org/10.1109/sc.2006.19

[10] Khatri, H. (2019). INDIONESIA Laporan Pengalaman Jaringan Seluler Juli 2019. [Online]. Available https://www.opensignal.com/in/reports/2019/07/indonesia/mobile-network-experience. Accessed on August 8, 2019