Abstrak

Metode *Clustering Storage* untuk Penyimpanan Bukti Digital Menggunakan *Software Defined Storage*

Meningkatnya *cybercrime* berarti meningkatnya pula kuantitas barang bukti digital yang dihasilkan dalam aktivitas kejahatan tersebut. Pembangunan tempat penyimpanan barang bukti digital (*digital evidence storage*) selain memperhatikan keamanan dan integritas data digital, juga perlu memperhatikan kebutuhan akan hal kemudahan dalam penambahan *storage* (skalabilitas) serta kebutuhan penyidik agar tidak terkendala masalah geografis dalam melaksanakan tugasnya. Impelementasi yang ideal dari permasalahan tersebut adalah pembangunan *digital evidence storage* berbasis *network* dengan penggunan *software defined storage* untuk membangun sistem *clustered storage*. Salah satu *software defined storage* yang memiliki skalabilitas yang sangat baik adalah Ceph. Ceph juga memiliki fitur *self-healed* dan *self-managed* yang membuat Ceph *reliable* dan *high-available*.

Dalam penelitian ini sistem *digital evidence storage* yang dibangun terdiri dari 8 node *server storage*, 2 *server* Ceph monitor (MON) dan 1 Ceph *client*. Setiap node *server storage* memiliki 2 buah OSD yang akan digabungkan dalam sebuah *storage cluster*. Setiap OSD memiliki kapasitas 20Gb. Selanjutnya Ceph *storage cluster* akan ditautkan dari *server* Ceph monitor ke Ceph *client*. Ceph *client* bertindak sebagai *server* yang akan diakses oleh penyidik menggunakan jaringan terenkripsi yaitu melalui jaringan kabel dan jaringan nirkabel (*wireless* maupun GSM). Pengujian dilakukan untuk menguji sistem dari kriteria skalabilitas, keamanan, integritas data serta availabilitas. Kriteria skalabilitas diuji dengan penambahan 2 node ke dalam sistem berjalan, hasilnya proses penambahan berlangsung aman tanpa gangguan. Kriteria keamanan diuji dengan metode *sniffing* (penyadapan) pada setiap paket yang melewati jaringan, hasilnya koneksi VPN dan penggunaan protokol https dalam penelitian ini membuat transmisi data terenkripsi. Dengan kata lain, kriteria keamanan data dalam sistem telah terpenuhi. Kriteria integritas data diuji dengan sinkronisasi file menggunakan jaringan GSM dalam beberapa kualitas koneksi dengan parameter *ping time*, *jitter*, besaran *bandwidth*, serta *packet loss* kemudian membandingkan hasil hashing MD5 file sumber dan file yang ter-*upload* di sistem. Dari pengujian tersebut, transfer *file* dengan *bandwidth* yang kecil atau kualitas jaringan yang kurang baik tidak mempengaruhi *integrity* file. Pengujian kriteria availabilitas dilakukan dengan membuat 4 node terputus saat dilakukan sinkronisasi file.

Dari hasil uji coba sistem *digital evidence storage* yang dibangun menggunakan Ceph telah memenuhi kriteria skalabilitas, availabilitas, keamanan serta integritas data, sehingga bukti digital yang disimpan dalam *digital evidence storage* yang dibangun dapat diajukan sebagai bukti di pengadilan.

Kata kunci

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

Abstract

Clustering Storage Method for Digital Evidence Storage Using Software Defined Storage

Increasing of cybercrime also means an increase in the quantity of digital evidence in these criminal activities. The making of digital evidence storage in addition to paying attention to the security and integrity of data, also needs to pay attention to the need for convenience in the addition of storage (scalability) and the needs of investigators so as not to be constrained by 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 make a clustered storage system. One of the software defined storage that has excellent scalability is Ceph. Ceph also has self-healed and self-managed features that make Ceph reliable and high-available.

In this study the digital evidence storage system that was built consisted of 8 storage server nodes, 2 Ceph monitors (MON) servers and 1 Ceph client. Each storage server node has 2 OSDs which will be combined in a storage cluster. Each OSD has a capacity of 20GB. 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 an encrypted network that is through a wired network and wireless network (wireless or GSM). Testing is run to test the system of scalability, security, data integrity and availability criteria. Scalability criteria are tested by adding 2 nodes into the running system, the result is that the addition process takes place safely without interruption. The security criteria were tested by sniffing method on every packet that passes through the network, the results were a VPN connection and the use of the https protocol technology in this study made encrypted data transmission. In other words, the data security criteria in the system have been met. Data integrity criteria were tested by synchronizing files using GSM networks in several connection qualities with parameters ping time, jitter, bandwidth, and packet loss then comparing the results of hashing MD5 source files and files uploaded on the system. From this test, file transfer with a small bandwidth or poor network quality does not affect file integrity. Availability testing criteria is done by making 4 nodes cut off during file synchronization process.

From the test results the digital evidence storage system that was built has met the criteria of scalability, availability, security and data integrity. Therefore, digital evidence which store in this storage system is valid and can be submitted as evidence in court.

Keywords

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