

## IMPLEMENTASI *PRIVATE CLOUD* MENGGUNAKAN METODE *ZERO TRUST* DAN *IP PUBLIC* DINAMIS PADA PT. ELNUSA SENTRA BAJATAMA

### IMPLEMENTATION OF *PRIVATE CLOUD* USING *ZERO TRUST* METHOD AND *DYNAMIC PUBLIC IP* AT PT. ELNUSA SENTRA BAJATAMA

Ahmad Raihan Mufid<sup>1</sup>, Kiki Setiawan<sup>2</sup>, Nandang Sutisna<sup>3</sup>

<sup>1,2,3</sup>Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Jakarta  
[ahmadraihan53@gmail.com](mailto:ahmadraihan53@gmail.com)<sup>1</sup>, [kid2djoaz@gmail.com](mailto:kid2djoaz@gmail.com)<sup>2</sup>

#### ABSTRACT

The development of information technology causes changes in company data storage. PT Elnusa Sentra Bajatama, which currently uses hard drives and flash drives, is vulnerable to data loss due to device damage and lack of good storage infrastructure. The purpose of this research is to implement Private Cloud Storage for a centralized data storage solution, as well as combining the concepts of Zero Trust and Dynamic Public IP to improve data security. The research data involves the number of users and office devices that will access cloud storage. This research uses the ROCCA approach with stages of analysis, planning, adoption, migration, and management. The results showed that the use of Nextcloud as a private cloud storage is successful in an enterprise environment, and the combination of Zero Trust and Dynamic Public IP is optimal in strengthening server security. Dynamic Public IP functions optimally in strengthening server security.

**Keywords:** Private Cloud Storage, Zero Trust, IP Public Dinamis, ROCCA

#### ABSTRAK

Perkembangan teknologi informasi menyebabkan perubahan signifikan dalam penyimpanan data perusahaan. PT. Elnusa Sentra Bajatama, yang bergerak di bidang penyedia alat rancak, saat ini menggunakan hardisk dan flashdisk pada komputer karyawan sebagai media penyimpanan. Namun, metode ini rentan terhadap kehilangan data akibat kerusakan perangkat dan tidak adanya infrastruktur penyimpanan yang memadai, sehingga memungkinkan akses tanpa izin terhadap data perusahaan. Penelitian ini bertujuan untuk mengimplementasikan *Private Cloud Storage* sebagai solusi penyimpanan data terpusat dan aman, dengan menggabungkan konsep *Zero Trust* dan *IP Publik Dinamis*. Data penelitian mencakup jumlah pengguna dan perangkat kantor yang akan mengakses *cloud storage*. Pendekatan ROCCA digunakan sebagai model implementasi sistem, meliputi tahapan analisis, perencanaan, adopsi, migrasi, dan pengelolaan. Hasil penelitian menunjukkan bahwa penggunaan Nextcloud sebagai *private cloud storage* berhasil diterapkan di lingkungan perusahaan. Kombinasi *Zero Trust* dan *IP Publik Dinamis* terbukti optimal dalam memperkuat keamanan akses server. Dapat disimpulkan bahwa implementasi ini menawarkan solusi efektif dan aman untuk penyimpanan data perusahaan, mengurangi risiko kehilangan data dan akses tanpa izin.

**Kata Kunci:** Private Cloud Storage, Zero Trust, IP Public Dinamis, ROCCA

#### PENDAHULUAN

Teknologi informasi telah menyebabkan perubahan signifikan dalam cara penyimpanan data perusahaan. Awalnya, perusahaan mengandalkan penyimpanan fisik seperti kertas dan lemari arsip, namun kini beralih ke penyimpanan digital yang lebih efisien dan fleksibel, salah satunya adalah *server storage*. *Server storage* adalah komponen kunci dalam infrastruktur teknologi informasi sebuah perusahaan, berfungsi sebagai tempat penyimpanan data yang

penting, menyediakan ruang untuk file, database, dan aplikasi yang diperlukan untuk menjalankan operasi sehari-hari. Namun, dengan kemajuan teknologi, konsep *server storage* telah berkembang menjadi infrastruktur yang lebih kompleks dan terintegrasi, termasuk penyimpanan awan (*cloud storage*). Berdasarkan survei, banyak lembaga publik di Indonesia masih belum menggunakan layanan *cloud storage* karena beberapa alasan, seperti kekhawatiran terhadap keamanan dan privasi data (55,1%), ketidakbutuhan

(34,7%), ketidakpastian aturan hukum (33,1%), terbatasnya anggaran investasi (31,4%), biaya besar (28,8%), kekurangan personel IT yang memahami layanan *cloud* (20,3%), dan kurangnya pengetahuan tentang layanan *cloud* (16,9%).

PT. Elnusa Sentra Bajatama adalah perusahaan penyedia alat perancah terkemuka yang saat ini menggunakan perangkat fisik seperti hard disk di komputer pribadi masing-masing karyawan untuk menyimpan data. Media penyimpanan ini rentan terhadap kerusakan yang dapat menyebabkan hilangnya data. Data-data perusahaan, termasuk data keuangan, legalitas, dan data penting lainnya, umumnya disimpan di komputer masing-masing karyawan, menyebabkan penyimpanan di komputer menjadi penuh sehingga performa komputer melambat. Selain itu, belum ada infrastruktur yang baik dalam konsep penyimpanan data, sehingga memungkinkan pengguna lain tanpa izin bisa mengakses data perusahaan. Oleh karena itu, diperlukan sistem penyimpanan *cloud* menggunakan virtual server untuk memastikan semua data perusahaan tersimpan dengan rapi dan terpusat dalam satu tempat.

Penggunaan metode *Zero Trust* dalam penyimpanan *cloud* telah menjadi pendekatan yang semakin populer untuk mengamankan data dan infrastruktur IT. Pendelegasian kepercayaan penting karena memungkinkan kita untuk membangun sistem otomatis yang dapat berkembang menjadi skala besar dan beroperasi dengan cara yang aman dan tepercaya dengan campur tangan manusia yang minimal (Gilman & Barth, 2017). Artinya, akses ke data dan sumber daya hanya diberikan ketika pengguna atau perangkat diautentikasi dan diotorisasi, tanpa kepercayaan pada entitas mana pun, termasuk pengguna atau perangkat internal yang terhubung dari luar jaringan. Dengan menerapkan *Zero Trust*, perusahaan dapat meningkatkan pertahanan mereka terhadap ancaman keamanan, mengurangi risiko

akses tidak sah atau pencurian data, dan meningkatkan keamanan penyimpanan *cloud* secara keseluruhan.

Penelitian yang dilakukan oleh Yuggo Afrianto, Ade Hendri Hendrawan tentang Implementasi Data Center Untuk Penempatan Host Server Berbasis *Private Cloud Computing*. Hasil penelitian adalah menganalisis sistem yang telah dibangun menunjukkan bahwa data center berbasis IaaS dapat menghemat, mengoptimalkan, dan mengelola sumber daya untuk memenuhi kebutuhan layanan sistem informasi yang harus diberikan kampus UIKA. Uji usability menunjukkan bahwa aplikasi proxmox memenuhi kebutuhan manajemen yang ada dari administrator IT kampus UIKA, termasuk pembelajaran, efisiensi, ingat, kesalahan, dan kepuasan. (Afrianto & Hendrawan, 2019).

Penelitian yang dilakukan oleh Waliadi Gunawan, Elan Sunandar tentang Implementasi *Cloud Storage* Menggunakan *Owncloud* dan Ubuntu Server Studi Kasus Pada PT Indonesia Nippon Seiki. Hasil penelitian yang didapat adalah Proses pertukaran file jarak jauh, seperti mengirim file lampiran berukuran lebih dari 5 MB, dapat diatasi dengan menggunakan layanan berbagi di *cloud storage*. Karena *Infrastructure cloud storage* seperti server dan media penyimpanan berada di dalam ruang lingkup bisnis, penyimpanan data di *cloud* dapat memberikan keamanan. Baik perancangan maupun implementasi sistem sudah dijadwalkan. Pihak IT akan membangun sistem, dan user terkait akan diberitahu tentangnya. (Gunawan & Sunandar, 2021)

Dalam penelitian yang dilakukan oleh Alfasyahri Zaki, Arya Pratama Damanik, Evan Alfian Syahnur, Harun Yahya, Muhammad Naufal Fathin Hibrizi, Rafli Khalis Nugraha tentang Implementasi *Cloud Computing* Berbasis Software as a Service (SaaS) Menggunakan *OwnCloud* Untuk Pengolahan Data Mahasiswa Sistem Informasi UINSU. Hasil yang didapat

adalah Perancangan arsitektur komputasi awan menggunakan model Software as a Service (SaaS) dan teknik adopsi model Roadmap Adoption *Cloud Computing* (ROCCA) menggunakan analisis SWOT untuk mengidentifikasi kebutuhan dalam rangka pengelolaan *Infrastructure*. Metode penerapan komputasi melalui tahapan analisis, perancangan, adopsi, migrasi, dan pengelolaan akan dirancang sesuai dengan model ROCCA. (Zaki et al., 2023)

Adapun tujuan dari penelitian ini adalah mengimplementasikan *private cloud storage* berbasis virtual server untuk memberikan solusi yang efektif terkait penyimpanan data perusahaan yang terpusat, serta mengkombinasikan konsep *Zero Trust* dan *IP Public* Dinamis dengan *cloud storage* untuk memberikan solusi terkait keamanan data yang terdapat dalam layanan *cloud*.

Maka dari permasalahan yang sudah diuraikan, membuat penulis tertarik untuk mengimplementasikan *private cloud* server pada PT. Elnusa Sentra Bajatama dan mengambil judul penelitian “Implementasi *Private Cloud Storage* Berbasis *Infrastructure* as a Service Menggunakan Metode *Zero Trust* dan *IP Public* Dinamis pada PT Elnusa Sentra Bajatama”.

**METODE**

**Data Penelitian**

Pengambilan data penelitian tersebut dilakukan secara kualitatif. Data kualitatif adalah data non-numerik atau angka. Penelitian ini terdiri dari data kualitatif yang diperoleh melalui beberapa metode:

1. **Data Primer:** data ini merujuk pada data yang dikumpulkan secara langsung oleh peneliti dari sumber aslinya.

**Observasi :** Peneliti melihat langsung terhadap keadaan yang terjadi pada perusahaan seputar *Infrastructure*, jumlah perangkat yang digunakan, jumlah user dan kebutuhan yang diperlukan.

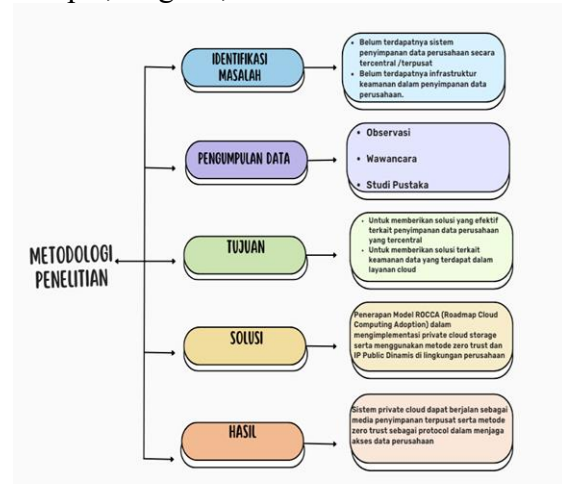
**Wawancara :** Peneliti melakukan tanya jawab dengan karyawan PT.Elnusa

Sentra Bajatama terkait kendala yang sering di hadapi untuk mendapatkan kesimpulan dan memberikan solusi dari permasalahan yang terjadi.

2. **Data Sekunder:** data yang dikumpulkan oleh pihak lain dan bukan langsung dari sumber pertama oleh peneliti yang saat ini menggunakannya. Biasanya, data ini telah dipublikasikan atau disediakan melalui berbagai media seperti laporan penelitian, buku, jurnal, dan database online.

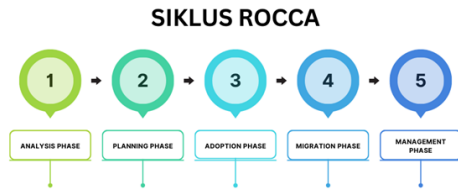
**Penerapan Metodologi**

Pada fase ini, peneliti akan melakukan penerapan metodologi dalam menerapkan Implementasi *Private Cloud Storage* menggunakan metode *Zero Trust* dan *IP Public* Dinamis di PT. Elnusa Sentra Bajatama. Fase pertama peneliti akan mengumpulkan data terlebih dahulu melalui observasi langsung dan sesi wawancara. Selanjutnya akan dilakukan pencatatan daftar nama pengguna serta data perangkat yang digunakan yang nantinya akan di daftarkan pada sistem *private cloud*. Peneliti juga membuat *Infrastructure* skema jaringan dalam implementasi *cloud storage*. Fase selanjutnya adalah penerapan metode ROCCA, dimana proses ini mengacu pada lima tahapan yaitu Analisis, Perancangan, Adopsi, Migrasi, Pemeliharaan.



**Gambar 1. Tahapan Penerapan Metodologi Rancangan Pengujian**

Rancangan pengujian menggunakan ROCCA (Roadmap *Cloud Computing* Adoption) bertujuan untuk menguji performa serta pengoptimalan kinerja *cloud* server dalam tahap siklus pengembangan. Adapun tahapan yang dilakukan dalam pengujian dapat terlihat pada gambar 2, sebagai berikut :



**Gambar 2. Siklus ROCCA**

- a. Analisis (Analysis Phase)
 

Pada tahap ini, pertama-tama dilakukan identifikasi kebutuhan penyimpanan data dan kapasitas yang dibutuhkan oleh PT. Elnusa Sentra Bajatama. Evaluasi dilakukan untuk melihat bagaimana solusi *Private Cloud* bisa diintegrasikan dengan infrastruktur IT yang sudah ada. Analisis risiko juga dilakukan untuk mengidentifikasi ancaman keamanan yang mungkin terjadi dengan metode *Zero Trust* serta risiko operasional dari penggunaan IP *Public* Dinamis. Selain itu, ditinjau juga kepatuhan terhadap regulasi dan standar industri.
- b. Perencanaan (Planning Phase)
 

Tahap ini melibatkan desain arsitektur solusi *Private Cloud* dengan metode *Zero Trust*, termasuk mekanisme autentikasi dan otorisasi serta integrasi IP *Public* Dinamis dalam jaringan. Infrastruktur jaringan yang mendukung *Private Cloud* juga dirancang, meliputi pemilihan perangkat keras dan perangkat lunak yang sesuai, serta solusi backup dan pemulihan data.
- c. Adopsi (Adoption Phase)
 

Pada tahap ini, dilakukan pelatihan untuk mengelola dan mengoperasikan *Private Cloud* serta memahami prinsip-prinsip *Zero Trust* dan manajemen IP *Public* Dinamis. Pelatihan juga diberikan kepada pengguna akhir tentang penggunaan dan keamanan data

di *Cloud*. Uji coba terbatas dilakukan pada beberapa departemen sebelum implementasi penuh, untuk memastikan performa, keamanan, dan reliabilitas solusi yang diusulkan. Manajemen perubahan mencakup komunikasi perubahan kepada seluruh staf dan manajemen, pembuatan dokumentasi lengkap tentang prosedur baru, serta penyediaan mekanisme dukungan untuk membantu transisi pengguna.

#### d. Migrasi (Migration Phase)

Tahap ini dimulai dengan persiapan rencana migrasi yang mencakup timeline, tugas, dan tanggung jawab yang jelas. Backup lengkap dilakukan sebelum migrasi dimulai. Pelaksanaan migrasi dilakukan secara bertahap untuk meminimalkan gangguan operasional, dengan verifikasi integritas dan konsistensi data setelah setiap tahap migrasi. Setelah migrasi, dilakukan tes akhir untuk memastikan semua sistem berfungsi dengan baik, pemantauan kinerja sistem untuk mengidentifikasi masalah, dan pengumpulan umpan balik dari pengguna untuk perbaikan lebih lanjut.

## HASIL DAN PEMBAHASAN

Dalam penelitian ini, data yang digunakan adalah data list perangkat beserta data user yang akan didaftarkan pada *Cloud Server*. Data tersebut akan digunakan dalam proses implementasi sistem menggunakan metode ROCCA. Proses Implementasi menggunakan metode ROCCA (Roadmap for *Cloud Computing* Adoption) memiliki lima tahapan yang akan dijelaskan sebagai berikut:

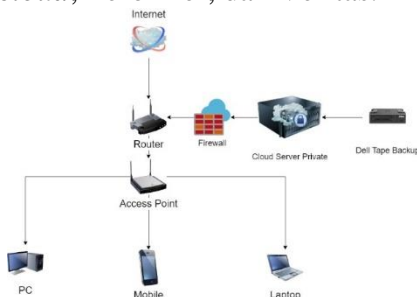
### Fase Analisis (Analysis Phase)

Tahap pertama adalah mengidentifikasi kebutuhan penyimpanan data dengan menentukan volume data saat ini, perkiraan pertumbuhannya, serta bagaimana data akan diakses, ketersediaan, dan durabilitasnya, termasuk kebutuhan backup dan pemulihan bencana.

Selanjutnya, evaluasi infrastruktur IT yang ada dilakukan untuk memastikan solusi *Private Cloud* dapat terintegrasi dengan baik, termasuk pemilihan jenis *cloud* dan perangkat penyimpanan yang kompatibel. Analisis risiko keamanan dilakukan untuk mengidentifikasi potensi ancaman dan memutuskan penggunaan Multi Factor Authenticator. Karena tidak tersedianya IP publik di PT Elnusa Sentra Bajatama, diperlukan penghubung agar server bisa diakses dari luar kantor dan dikombinasikan dengan konsep *Zero Trust*.

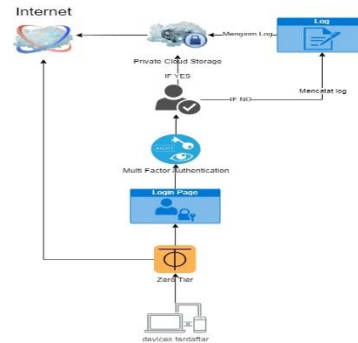
**Fase Perencanaan (Planning Phase)**

Dalam fase ini, infrastruktur yang akan digunakan ditentukan, termasuk pemilihan server fisik, perangkat jaringan, dan tape untuk backup. Sistem operasi yang digunakan adalah Linux (Ubuntu Server) dengan perangkat lunak seperti *Nextcloud*, *Zero Tier*, dan *Veritas*.



**Gambar 3. Evaluasi Infrastruktur Jaringan**

Infrastruktur *cloud* server akan menggunakan *Nextcloud*, dengan pengaturan pengguna, grup, hak akses, dan integrasi Multi Factor Authenticator. Hard disk berukuran 100GB digunakan untuk penyimpanan data selama penelitian. Backup dilakukan mingguan menggunakan *Veritas* dan tape. *Zero Tier* diinstal untuk mengelola IP dinamis dan memastikan akses data melalui jaringan virtual ini, dikombinasikan dengan multi-factor authentication. Akses ke server hanya melalui *Zero Tier*, dengan perangkat yang terdaftar, dan aktivitas dipantau secara aktif dengan logging dan deteksi insiden real-time.



**Gambar 4. Perencanaan Infrastruktur Keamanan Server Fase Adopsi (Adoption Phase)**

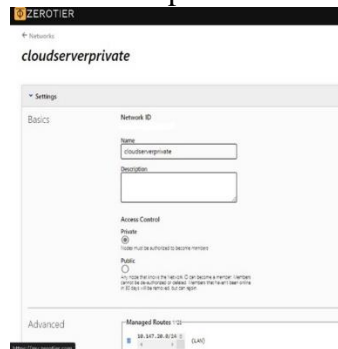
Tahap implementasi perangkat lunak di PT Elnusa Sentra Bajatama dimulai dengan menginstal Host Operating System (Windows 10 Pro) dan Guest Operating System (Ubuntu Server 22.04) di VMWare Workstation. Di Ubuntu, diinstal LAMP untuk mendukung *Nextcloud* yang dikonfigurasi dengan database *MariaDB*.

```

installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/drs/2020-02-26/paginac
es-1.json.php
installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/drs/2020-02-26/api-2.js
on.php
installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/drs/2020-02-26/endpoint
-rule-set-1.json.php
creating: nextcloud/3rdparty/ava/ava-sdk-php/src/data/networkmanager/
creating: nextcloud/3rdparty/ava/ava-sdk-php/src/data/networkmanager/2019-07-
05/
installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/networkmanager/2019-07-
05/paginators-1.json.php
installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/networkmanager/2019-07-
05/eps-2.json.php
installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/networkmanager/2019-07-
05/endpoint-rule-set-1.json.php
creating: nextcloud/3rdparty/ava/ava-sdk-php/src/data/quaradaty/
creating: nextcloud/3rdparty/ava/ava-sdk-php/src/data/quaradaty/2017-11-28/pa
ginator-1.json.php
installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/quaradaty/2017-11-28/pa
ginator-1.json.php
installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/quaradaty/2017-11-28/ep
s-2.json.php
installing: nextcloud/3rdparty/ava/ava-sdk-php/src/data/quaradaty/2017-11-28/en
dpoint-rule-set-1.json.php
creating: nextcloud/3rdparty/ava/ava-sdk-php/src/data/11a/
    
```

**Gambar 5. Install Nextcloud**

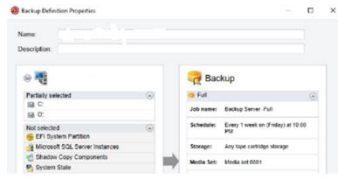
Selanjutnya, *Zero Tier* diatur untuk manajemen IP dan akses sesuai dengan konsep *Zero Trust*, memastikan semua perangkat yang mengakses terdaftar dan divalidasi. Virtual server dihubungkan ke *Zero Tier*, dan validasi perangkat dilakukan melalui platform *Zero Tier*.



**Gambar 6. Konfigurasi Zero Tier**

Implementasi backup dilakukan menggunakan tape backup dan *Veritas*, dengan backup dijadwalkan setiap Jumat. Rencana pemulihan bencana mencakup skenario bencana, RPO, dan RTO.

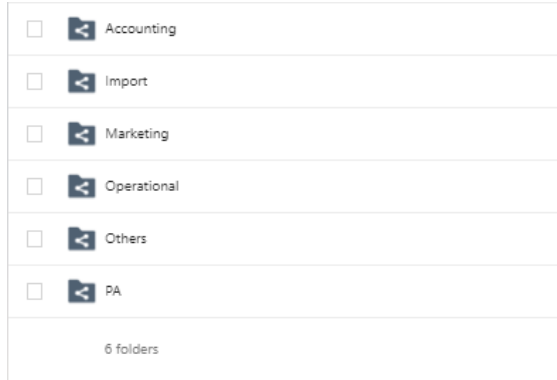
Terakhir, akses local IP ke *cloud* server dinonaktifkan untuk memastikan keamanan akses.



**Gambar 7. Konfigurasi Backup Server**

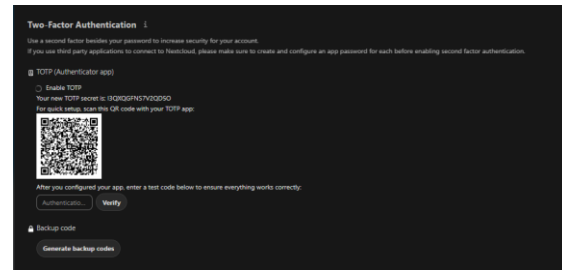
**Fase Migrasi (Migration Phase)**

Langkah awal fase migrasi adalah pembuatan user yang akan mengakses *cloud* server tersebut berdasarkan data penelitian yang sudah di kumpulkan sebelumnya, user tersebut akan di kelompokkan berdasarkan departemen dan di tentukan quota per masing-masing user. Lalu berikutnya adalah pembuatan folder per department, yang dimana setiap folder hanya bisa diakses oleh department tertentu saja sesuai dengan hak akses yang diberikan oleh administrator.



**Gambar 8. Folder Departement**

Perangkat user dihubungkan ke sistem Zero Tier untuk validasi, dan Multi Factor Authentication diaktifkan menggunakan Google Authenticator. Migrasi dilakukan bertahap untuk mengurangi gangguan, dengan verifikasi integritas dan konsistensi data setelah setiap tahap.



**Gambar 9. Enable Multi Factor Authentication**

**Fase Pemantauan (Monitoring Phase)**

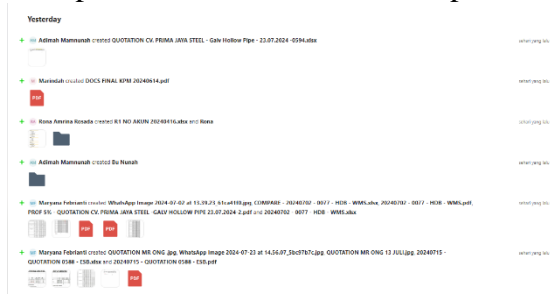
Tahap pengelolaan dan monitoring setelah migrasi mencakup pengawasan kinerja dan keamanan sistem secara real-time, jadwal pemeliharaan rutin untuk update dan perbaikan, serta tim respons insiden untuk menangani masalah keamanan atau operasional. Keamanan ditingkatkan dengan update dan patch berkala, audit keamanan rutin, dan peninjauan kebijakan keamanan. Evaluasi kinerja sistem dilakukan secara berkala untuk memastikan pemenuhan kebutuhan bisnis dan rencana upgrade teknologi disusun agar solusi *Private Cloud Storage* tetap optimal dan relevan.

**Hasil Akhir Pengujian**

Setelah seluruh tahapan perencanaan, migrasi, dan pengelolaan selesai dilaksanakan, berbagai hasil dan pengujian dilakukan untuk memastikan keberhasilan implementasi solusi *Private Cloud Storage* dengan metode *Zero Trust* dan IP Publik Dinamis. Hasil awal menunjukkan bahwa server fisik dan perangkat lunak berfungsi dengan baik, dan sistem operasi Ubuntu Server berhasil diinstal tanpa kendala. Instalasi dan konfigurasi *Nextcloud* juga berjalan lancar, dengan pengguna dan grup yang telah diatur serta sistem autentikasi yang terintegrasi dengan baik.

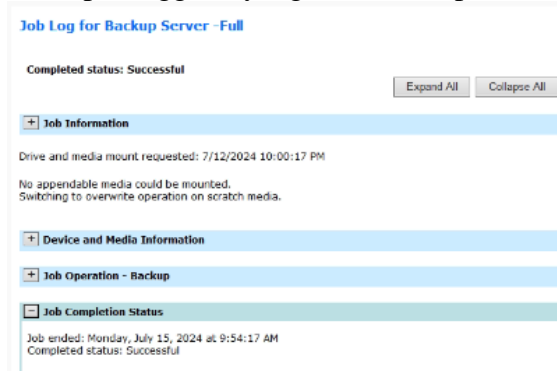
Proses migrasi data existing ke *Nextcloud* berhasil dilakukan secara bertahap, dengan verifikasi integritas dan konsistensi data setelah setiap tahap migrasi menunjukkan bahwa tidak ada data yang hilang atau rusak. Ukuran hardisk sebesar 100GB terbukti cukup

untuk menampung data yang dimigrasikan serta pertumbuhan data di masa depan.



**Gambar 10. Proses Migrasi Data**

Implementasi solusi backup menggunakan tape backup dan software Veritas berhasil dilaksanakan sesuai jadwal. Pengujian backup dan pemulihan data menunjukkan bahwa data dapat dibackup dan dipulihkan dengan sempurna, sesuai dengan strategi full backup mingguan yang telah ditetapkan.



**Gambar 11. Proses Backup Cloud**

Konsep *Zero Trust* dapat diterapkan dengan sukses dengan dilakukan pengujian terhadap perangkat yang tidak diberikan izin pada console Zero Tier dalam upaya pengaksesan *cloud server*. Zero Tier berhasil di install dan dapat dikonfigurasi untuk mengelola IP *Public* Dinamis Akses IP lokal ke *cloud server* dinonaktifkan.

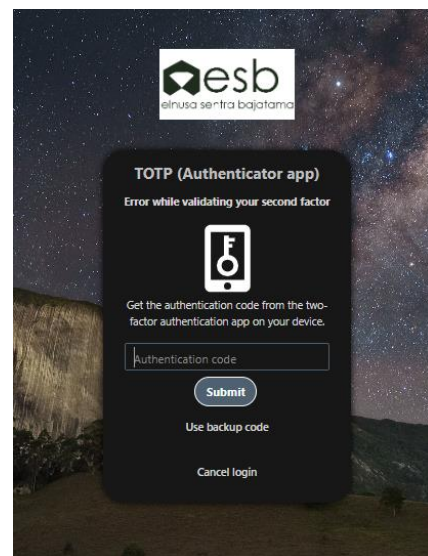


**Gambar 11. Uji Testing pada perangkat yang tidak terverifikasi**



**Gambar 12. Percobaan akses cloud server melalui IP Local**

Pengujian juga dilakukan pada multi-factor authentication (MFA) menggunakan Google Authenticator. Jika terdapat aktivitas mencurigakan maupun kesalahan input code pada MFA, maka log akan mencatat hal tersebut dan user tidak dapat mengakses ke dalam server.



**Gambar 12. Pengujian Multi Factor Authentication**



**Gambar 12. Log Aktivitas Login user**

## SIMPULAN

Berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa penggunaan *private cloud storage* dapat dilakukan di lingkungan perusahaan maupun organisasi khususnya di PT. Elnusa Sentra Bajatama. Data user serta

data infrastruktur secara baik dapat digunakan dalam membantu penulis menyelesaikan penelitian ini.

Berdasarkan penelitian yang dilakukan di PT. Elnusa Sentra Bajatama, maka dapat diambil kesimpulan sebagai berikut:

- a. Implementasi solusi *Private Cloud Storage* dengan metode *Zero Trust* telah berhasil dilaksanakan dengan baik melalui tahapan perencanaan yang matang, migrasi yang terstruktur, dan pengelolaan yang komprehensif. Infrastruktur yang dipilih, termasuk perangkat keras dan perangkat lunak yang mendukung, telah memastikan fondasi yang kuat bagi sistem. *Nextcloud* sebagai *cloud server* diinstal dan dikonfigurasi dengan lancar, memberikan platform penyimpanan yang aman dan terkelola dengan baik.
- b. Penggunaan konsep *Zero Trust* dan IP *Public* Dinamis dalam sebuah *Private Cloud Storage* dapat membantu dalam pengamanan akses yang efektif serta memastikan keamanan data sulit untuk di bobol.

#### DAFTAR PUSTAKA

- Afrianto, Y., & Hendrawan, A. H. (2019). Implementasi Data Center Untuk Penempatan Host Server Berbasis *Private Cloud Computing*. *Krea-Tif*, 7(1), 50. <https://doi.org/10.32832/kreatif.v7i1.2031>
- Gilman, E., & Barth, D. (2017). *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media. <https://books.google.co.id/books?id=eawoDwAAQBAJ>
- Gunawan, W., & Sunandar, E. (2021). Implementasi *Cloud Storage* Menggunakan *Owncloud* Dan *Ubuntu Server* Studi Kasus Pada Pt Indonesia Nippon Seiki. *Journal of Innovation And Future Technology (IFTECH)*, 3(1), 1–10. <https://doi.org/10.47080/iftech.v3i1.1143>

Zaki, A., Damanik, A. P., Syahnur, E. A., Yahya, H., Naufal, M., Hibrizi, F., & Khalis Nugraha, R. (2023). Implementasi *Cloud Computing* Berbasis Software as a Service (SaaS) Menggunakan *OwnCloud* Untuk Pengolahan Data Mahasiswa Sistem Informasi UINSU. *Jurnal Komputer Teknologi Informasi Sistem Komputer*, 1(3), 179–184.