Journal of Digital Business and Technology Innovation (DBESTI)

https://journal.nurulfikri.ac.id/index.php/DBESTI
P-ISSN: 3047-1028 E-ISSN: 3032-775X

MODEL INFRASTRUKTUR *BACKUP DATA* MENGGUNAKAN NAS UNTUK MENUNJANG KEBERLANGSUNGAN SISTEM INFORMASI PERUSAHAAN

Iqbal Naveliano[1], Suhendi[2]

[1,2] Sistem Informasi, Sekolah Tinggi Teknologi Terpadu Nurul Fikri
Jakarta Selatan, DKI Jakarta, Indonesia 12640
iqba20111si@nurulfikri.ac.id, suhendi@nurulfikri.ac.id

Abstract

The rampant cyber attacks that have hit Indonesian cyberspace recently have resulted in data loss in several companies. The cyber attacks that occurred are hazardous to company data. In 2022, the company PT. Global Media Utama Teknologi experienced a ransomware cyber attack that resulted in data loss and caused losses to the company. This incident requires a solution to prevent data loss from occurring again due to cyber attacks or accidents in company operations. In this study, a data backup infrastructure design was implemented at PT. Global Media Utama Teknologi uses several technologies, such as Network Attached Storage (NAS) and backup applications from Acronis Cyber Protect. This study was tested at the end using Black Box Testing, User Acceptance Testing (UAT), Backup Testing, and Restore Testing. The results of the study show that the backup infrastructure design at PT is Global Media Utama Teknologi has run according to user wishes.

Keywords: *Backup, Information Systems, NAS, Ransomware, Restore*

Abstrak

Maraknya serangan siber yang menimpa ruang siber Indonesia beberapa waktu ini, mengakibatkan terjadinya kehilangan data pada beberapa perusahaan. Jelas, serangan siber yang terjadi sangat membahayakan data perusahaan. Pada tahun 2022, perusahaan PT. Global Media Utama Teknologi mengalami penyerangan siber *ransomware* yang mengakibatkan hilangnya data dan membuat kerugian pada perusahaan. Dari kejadian tersebut, dibutuhkannya solusi untuk mencegah terjadinya kembali kehilangan data akibat dari serangan siber ataupun ketidaksengajaan dalam operasional perusahaan. Dalam penelitian ini, dilakukan implementasi rancangan infrastruktur *backup data* di PT. Global Media Utama Teknologi dengan menggunakan beberapa teknologi, seperti *Network Attached Storage (NAS)* dan aplikasi *backup* dari perusahaan *Acronis Cyber Protect*. Penelitian ini diuji akhir dengan menggunakan *Black Box Testing, User Acceptence Testing* (UAT), *Backup Testing*, dan *Restore Testing*. Hasil penelitian menunjukkan bahwa rancangan infrastruktur *backup* di PT. Global Media Utama Teknologi telah berjalan sesuai dengan keinginan pengguna.

Kata kunci: *Backup*, NAS, *Ransomware*, *Restore*, Sistem Informasi

1. PENDAHULUAN

Saat pertama kali ditemukan komputer hanyalah sebuah mesin besar dengan kemampuan yang terbatas, dalam waktu yang singkat piranti tersebut telah mengalami perkembangan yang signifikan baik dari sisi kemampuan maupun ukuran. Banyak perusahaan menggunakan komputer dalam aktivitas hariannya, begitu pula dengan pemakai perseorangan. Terlebih lagi sejak ditemukannya internet pada tahun 1969 dan mengalami *booming* seperempat abad kemudian. Internet telah memberikan dampak yang jauh lebih besar pada komunikasi berbasis komputer daripada perkembangan yang lain, dan pula dilakukannya transaksi bisnis via Internet. Perusahaan-perusahaan berskala dunia semakin banyak memanfaatkan fasilitas internet. Sementara itu tumbuh transaksi-transaksi melalui elektronik atau *on-line* dari berbagai sektor, yang kemudian memunculkan istilah: *e-banking, ecommerce, e-trade, e-business, e-government, education* dan *e-retailing.* Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. [1]

Di satu sisi teknologi informasi dapat memberikan manfaat, mempermudah dan mempercepat akses informasi yang kita butuhkan dalam segala hal serta dapat mengubah model perekonomian dan model berbisnis. Namun dampak negatif

Diterima 6 Agustus 2024, Direvisi 28 Mei 2025, Diterima untuk publikasi 30 Mei 2025

pun tidak bisa dihindari. Seiring perkembangan teknologi internet, menyebabkan munculnya kejahatan baru yang disebut dengan *new cybercrime* melalui jaringan internet. Munculnya beberapa kasus *cybercrime* di Indonesia, seperti penipuan, *hacking*, penyadapan data orang lain, *spaming* email, dan manipulasi data dengan program komputer untuk mengakses data milik orang lain. Kejahatan-kejahatan yang ditimbulkan oleh pelaku *cybercrime* telah merugikan dalam jumlah besar bagi korbannya serta perekonomian dan martabat bangsa Indonesia di mata dunia. Untuk penanggulangan permasalahan kejahatan internet ini diperlukan Lembaga-lembaga khusus, baik milik pemerintah maupun NGO (Non *Government Organization*). Di Indonesia telah memiliki IDCERT (Indonesia *Computer Emergency Rensponse Team*). Unit ini merupakan point of contact bagi orang untuk melaporkan masalah-masalah keamanan komputer, namun perlu mendapat dukungan dari semua pihak agar misi-misinya cepat tercapai. [2]

Pada tahun 2022 bulan November PT. Global Media Utama Teknologi terkena serangan *ransomware* yang mengakibatkan seluruh data hilang dan terenkripsi. Pada saat terkena serangan *ransomware* PT. Global Media Utama Teknologi tidak memiliki adanya *backup* yang mengakibatkan seluruh operasional perusahaan terhenti, dan mengalami kerugian yang cukup besar. Dengan adanya kejadian tersebut PT. Global Media Utama Teknologi menginginkan adanya sebuah solusi *backup* yang bisa melindungi data perusahaan dari serangan *ransomware* atau kehilangan data lainnya. Oleh karena itu terpilih sebuah solusi aplikasi *backup data* dari perusahaan *Acronis* dengan nama aplikasi *backup data*-nya *Acronis cyber protect*. Aplikasi *acronis cyber protect* memilik sebuah fitur yang dapat menjadi solusi dari permasalahan yang di hadapi oleh PT. Global Media Utama teknologi, seperti *backup* secara otomatis, fitur anti-virus yang di mana dapat melakukan *scanning* terhadap *file* yang akan dilakukan *backup*, selanjutnya *acronis cyber protect* juga bisa melakukan *cloud backup* di AWS S3. Tidak lupa juga PT. Global Media Utama Teknologi menjadikan TrueNAS sebagai tempat penampung dari hasil *backup* yang sudah dilakukan oleh aplikasi *acronis cyber protect.*

2. METODE PENELITIAN

Pada bagian ini berisi penjelasan tentang jenis penelitian/desain penelitian.

2.1 Metode Analisis

Metode analisis yang dilakukan yaitu menggunakan metode pendekatan kualitatif melalui observasi langsung terhadap lokasi penelitian, dan mendengarkan langsung mengenai permasalahan pada lokasi penelitian, kebutuhan pengguna, uji fungsionalitas, dan uji *backup*, dengan melakukan percobaan *restore* terhadap data yang sudah di lakukan *backup*.

1. Observasi
   Peneliti melakukan observasi terhadap lokasi yang akan menjadi tempat penelitian, apakah lokasi tersebut memiliki permasalahan yang dapat diselesaikan dengan solusi dari penulis.

2. Studi Pustaka
   Proses ini dilakukan dengan tujuan untuk mendapatkan informasi dan data dari berbagai informasi, termasuk dokumen-dokumen seperti buku, jurnal, dokumentasi, dan berbagai bentuk digital lainnya.

Dalam metode pengumpulan data saat pengujian rancangan infrastruktur *backup data* yang sudah diimplementasikan digunakan pendekatan *Black Box Testing*, *User Acceptance Testing* (UAT*). Black box testing* bertujuan untuk memastikan bahwa fungsionalitas eksternal aplikasi sesuai dengan spesifikasi dan kebutuhan pengguna tanpa memperhatikan detail implementasinya. *UAT* dilakukan oleh pengguna akhir untuk memastikan rancangan infrastruktur *backup data* yang sudah di implementasikan dapat berjalan sesuai dengan harapan.

Rancangan infrastruktur teknologi informasi

Rancangan infrastruktur teknologi informasi melibatkan perencanaan dan pengorganisasian komponen teknis seperti perangkat keras, perangkat lunak, jaringan, dan penyimpanan data untuk mendukung kebutuhan bisnis. Tujuan utamanya adalah menciptakan sistem yang efisien, *scalable*, dan aman. Rancangan ini mencakup identifikasi kebutuhan bisnis, pemilihan teknologi yang sesuai, desain arsitektur sistem, serta perencanaan implementasi dan pemeliharaan. [3]

Infrastruktur jaringan

Infrastruktur jaringan adalah komponen fisik dan logis yang mendukung komunikasi dan interkoneksi antara perangkat dalam suatu organisasi. Ini meliputi topologi jaringan, protokol komunikasi, peralatan jaringan seperti *router* dan *switch*, serta keamanan jaringan. Infrastruktur yang baik harus dapat mendukung ketersediaan tinggi, kecepatan transmisi data yang memadai, dan keamanan dari ancaman eksternal maupun internal. [4]

Sistem Informasi

Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengelolaan, transaksi harian, mendukung operasi, bersifat manajerial, dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang dibutuhkan. [5]

Backup

Backup adalah proses membuat data cadangan dengan cara menyalin atau membuat arsip data komputer sehingga data tersebut dapat digunakan kembali apabila terjadi kerusakan atau kehilangan. [6]

Metodologi *Backup*

Metodologi *backup* serangkaian langkah dan prosedur terstruktur untuk membuat dan memelihara salinan data yang aman. Metodologi ini berperan penting dalam melindungi data dari kehilangan atau kerusakan, serta memastikan pemulihan data yang cepat dan mudah jika diperlukan. [7]

Incremental Backup

Incremental backup hanya mencadangkan data yang telah berubah sejak pencadangan terakhir, baik itu pencadangan penuh atau *incremental* sebelumnya. Metode ini menghemat ruang penyimpanan dan waktu pencadangan karena hanya menyimpan perubahan terkini. Namun, pemulihan data dari *incremental backup* bisa lebih kompleks karena memerlukan urutan semua *backup* sebelumnya untuk memulihkan data secara lengkap. [8]

Differential Backup

Differential backup mencadangkan semua data yang telah berubah sejak *full backup* terakhir. Berbeda dengan *incremental backup*, *differential backup* tidak memperhitungkan perubahan dari *backup differential* sebelumnya. Ini berarti bahwa setiap *differential backup* berisi semua perubahan sejak *full backup*, yang mempermudah pemulihan karena hanya membutuhkan *full backup* dan *differential backup* terbaru. Namun, *differential backup* cenderung memerlukan lebih banyak ruang penyimpanan dibanding *incremental backup* karena data yang dicadangkan semakin banyak seiring waktu. [8]

Full Backup

Full backup adalah metode pencadangan di mana seluruh data dari sistem atau perangkat disalin dan disimpan pada lokasi cadangan yang ditentukan. Ini adalah bentuk pencadangan paling lengkap, karena mencakup semua *file* dan direktori. Keuntungan utama dari *full backup* adalah kemudahan pemulihan karena semua data ada di satu tempat. Namun, *full backup* memerlukan ruang penyimpanan yang besar dan waktu pencadangan yang lama, terutama jika data yang dicadangkan berukuran besar. [8]

Acronis Cyber Protect

Acronis sebuah perusahaan teknologi global yang berkantor pusat di Swiss dan Singapura, didirikan pada tahun 2003. Acronis fokus pada solusi *cyber protection* yang terintegrasi untuk data, aplikasi, dan sistem. [9]

Acronis Cyber Protect (sebelumnya dikenal sebagai *Acronis True Image*) adalah paket perangkat lunak yang diproduksi oleh *Acronis International GmbH* yang bertujuan untuk melindungi sistem dari *ransomware* dan memungkinkan pengguna membuat *backup* dan *recovery file* atau seluruh sistem dari *backup*, yang sebelumnya dibuat menggunakan perangkat lunak. [10]

PT. Global Media Utama Teknologi

PT. Global Media Utama Teknologi sebuah perusahaan yang bergerak di bidang teknologi informasi komunikasi. PT. Global Media Utama Teknologi didirikan pada tahun 2009 dan beralamat di JL. Gunung Sahari Raya No.26, kelurahan gunung Sahari Utara, kecamatan sawah besar, kota Jakarta Pusat, provinsi DKI Jakarta, 10720. [11]

Ransomware

Ransomware adalah jenis perangkat lunak berbahaya (*malware*) yang dirancang untuk mengenkripsi data pada sistem komputer atau perangkat lainnya, dan kemudian menuntut pembayaran tebusan (*ransom*) kepada korban agar data tersebut dapat dikembalikan atau didekripsikan. [12]

Black box Testing

Pengujian *black box* adalah proses pengujian perangkat lunak yang membutuhkan pengujian aplikasi tanpa mengetahui kode program atau struktur internal aplikasi. [13]

UAT (*User Acceptance Testing)*

User Acceptance Testing merupakan pengujian yang dilakukan oleh *end user* yang langsung berinteraksi dengan sistem dan dilakukan verifikasi apakah fungsi yang ada telah berjalan sesuai dengan kebutuhan/fungsinya. *User Acceptance* Testing menguji yang dilakukan oleh pengguna sistem. Hasil dari pengujian dapat dijadikan bukti bahwa sistem dapat membantu para pengguna. *User Acceptance Testing* dilakukan pada pengembangan perangkat lunak bertujuan untuk memastikan sistem memenuhi kebutuhan sebenarnya dari pengguna, bukan hanya spesifikasi sistem. [14]

NAS (*Network Attached Storage)*

Network Attached Storage (NAS) adalah sebuah media penyimpanan jaringan yang dapat berupa sebuah *dedicated hardware* atau dapat pula berupa media penyimpanan yang dibangun dari sebuah komputer. [15]

TrueNAS

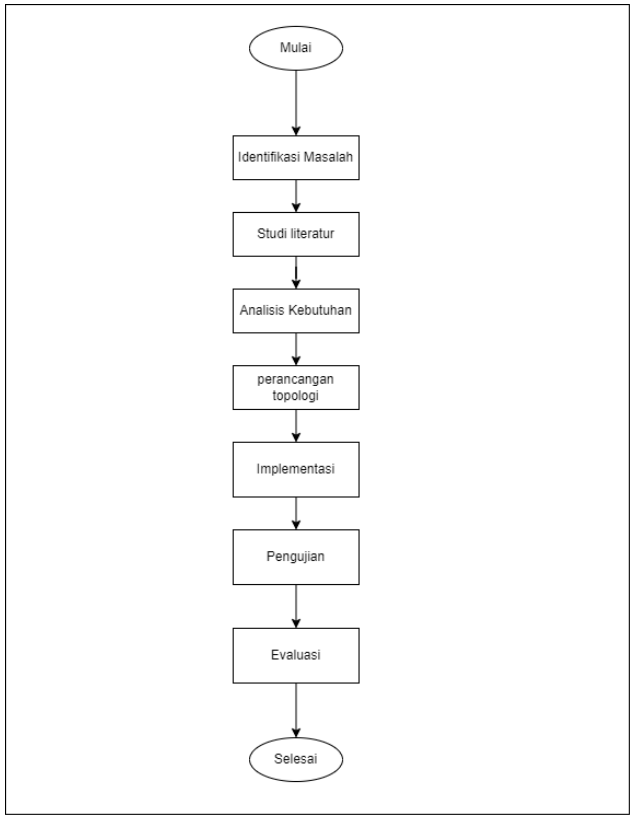
TrueNAS adalah sistem operasi penyimpanan terpasang jaringan (NAS) gratis dan sumber terbuka yang diproduksi oleh *iXsystems.* TrueNAS memiliki tiga versi. TrueNAS *CORE* adalah versi publik gratis, yang sebelumnya dikenal sebagai FreeNAS. TrueNAS *Enterprise* adalah edisi berlisensi *CORE* untuk Dukungan Perusahaan. TrueNAS *CORE* didasarkan pada FreeBSD. TrueNAS *SCALE* adalah TrueNAS *versi Linux* yang menghadirkan fitur tambahan seperti *container* dan *clustering Linux.* [16]

SMB(*Server Message Block)*

Server Message Block (SMB) adalah protokol komunikasi yang digunakan untuk berbagi *file*, printer, *port* serial, dan komunikasi lain-lain antar *node* di jaringan. [17]

2.2 Tahapan Penelitian

Pada tahapan ini penulis memberikan gambaran bagaimana langkah-langkah penulis dalam menyusun penelitian dari awal sampai dengan akhir. Dengan menyusun tahapan penelitian penulis dapat memastikan penelitian berjalan secara terstruktur dan sistematis, selanjutnya berikut penulis membuat alur diagram penelitian pada gambar 1 berikut.



Gambar 1. Tahapan Penelitian

Identifikasi masalah pada saat ini PT. Global Media Utama Teknologi belum memiliki sebuah infrastruktur *backup* yang bisa menunjang operasional perusahaan, dimana sangat rentan sekali terjadinya kehilangan data perusahaan yang akan berdampak pada operasional perusahaan. Berdasarkan permasalahan tersebut penulis menganalisis kebutuhan untuk membangun infrastruktur *backup* yang memungkinkan *backup* PT. Global Media Utama Teknologi bisa berjalan secara otomatis dan terjadwal serta meminimalisir terjadinya kehilangan data.

Studi literatur tahapan ini melakukan pembelajaran pada Pustaka yang terkait dengan penelitian yang sedang di lakukan dan juga memahami teori-teori dasar yang berkaitan langsung dengan penelitian ini. Sumber pembelajaran yang di gunakan meliputi skripsi, jurnal ilmiah, artikel, dan arahan dari dosen pembimbing.

Analisis kebutuhan pada tahapan ini penulis melakukan analisa dari masalah-masalah yang sudah di temukan dan diidentifikasi, sehingga penulis mendapatkan apa saja yang dibutuhkan untuk melakukan perancangan infrastruktur *backup data* di PT. Global Media Utama Teknologi, yang kemudian akan di implementasikan menjadi sebuah sistem *backup*.

Perancangan topologi pada tahapan ini penulis melakukan perancangan topologi perangkat komunikasi dan informasi PT. Global Media Utama Teknologi, agar memudahkan penulis melakukan implementasi dan tidak mengganggu operasional perusahaan yang sedang berjalan. Perancangan ini juga menjadi dasar untuk sistem akan beroperasi.

Implementasi pada tahapan ini dilaksanakan proses implementasi rancangan infrastruktur *backup* yang sudah di analisa kebutuhan sebelumnya, Pada tahap ini penulis menggunakan aplikasi pendukung untuk memenuhi kebutuhan-kebutuhan yang sudah di analisa. Selanjutnya penulis menerapkan rancangan *backup* dengan rancangan pada gambar 2 berikut.

Gambar 2. Rancangan *Backup*

Rancangan *backup* penulis terdiri dari beberapa proses di antaranya:

1. Perencanaan dan Persiapan

Pada tahap ini kita melakukan perencanaan dan persiapan untuk memahami kebutuhan serta mempersiapkan apa saja yang harus dilakukan. Pada tahap ini segala kebutuhan wajib dilakukan pencatatan agar saat melakukan perencanaan tidak adanya kesalahan atau kekurangan sumber daya yang dibutuhkan saat implementasi. Persiapan juga mencakup jadwal *backup* akan dilakukan, perangkat penampung *backup*, aplikasi *backup*, dan juga server pengontrol aplikasi *backup*.

2. Identifikasi Data dan Kebutuhan *Backup*

Pada tahap ini dilakukannya identifikasi dan pencatatan data yang akan dilakukan *backup* serta menghitung jumlah total data yang akan di-*backup*. Selanjutnya setelah berhasil mendapatkan jumlah total data yang akan di *backup* maka kita akan menghitung kebutuhan *backup* dan menyiapkan tempat penampung hasil *backup*.

3. Menentukan Strategi *Backup*

Pada tahap ini penentuan strategi *backup* seperti jadwal *backup*, metodologi *backup*, *retention policy*, kompresi hasil *backup*.

4. Implementasi dan Memantau Strategi *Backup*

Pada tahap ini adalah implementasi *backup* dari penentuan strategi yang sudah ditentukan sebelumnya, dan ditahap ini juga pemantauan strategi *backup* yang sudah ditentukan sebelumnya.

5. Pengujian *Recovery Data* yang sudah di-*Backup*

Pada tahap ini pengujian *recovery data* yang sudah berhasil di-*backup* pada implementasi.

6. Memastikan Hasil *Backup* Tetap Konsisten

Pada tahap ini memastikan hasil *backup* tetap konsisten tidak adanya kehilangan data atau kerusakan data yang akan berdampak pada proses *recovery*.

Pengujian pada tahapan ini penulis melakukan pengujian terhadap hasil dari implementasi rancangan infrastruktur *backup*, apakah *backup* berjalan sebagaimana mestinya, dan apakah data yang sudah di-*backup* dapat di kembalikan jika terjadi kehilangan data.

Evaluasi pada tahapan ini penulis melakukan evaluasi terhadap implementasi rancangan infrastruktur *backup* apakah sudah sesuai dengan kebutuhan PT. Global Media Utama Teknologi, tapi jika belum maka penulis akan melakukan analisa Kembali terkait kebutuhan infrastruktur *backup* di PT. Global Media Utama Teknologi.

3. HASIL DAN PEMBAHASAN

Pada bagian ini berisi penjelasan hasil dan pembahasan mengenai analisis sistem, perancangan sistem. Ada beberapa diagram yang digunakan seperti desain topologi, serta tampilan dari aplikasi *Acronis Cyber Protect.*

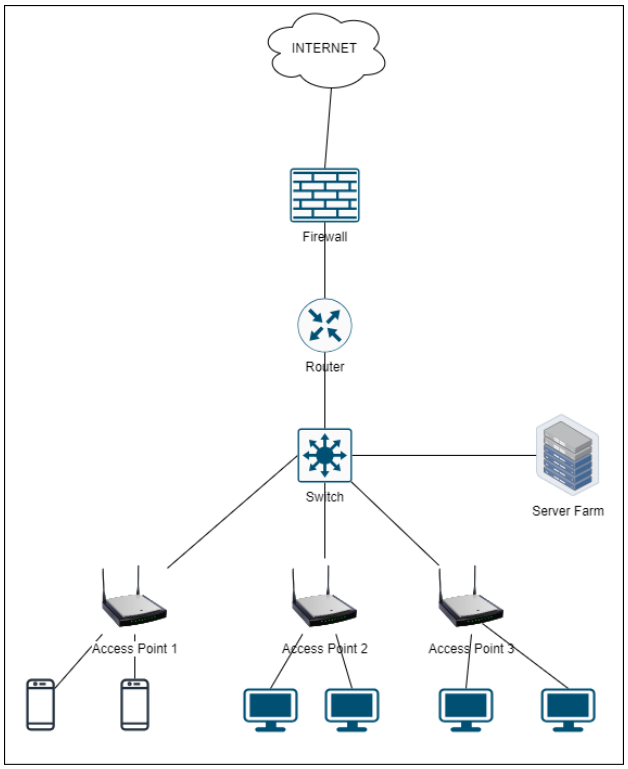
3.1. Analisis Sistem

Analisis sistem adalah cara suatu proses yang dilakukan untuk memahami, mengevaluasi dan memahami struktur, fungsi, dan kinerja suatu sistem. Dalam implementasi rancangan infrastruktur *backup data* di PT. Global Media Utama Teknologi, analisis sistem sangat penting untuk memahami masalah, kebutuhan, dan peluang yang dapat diatasi oleh implementasi rancangan infrastruktur *backup*.

Pada tahap ini akan dilakukan analisis jaringan infrastruktur yang sudah berjalan saat ini, kebutuhan *data* yang akan di *backup*, dan keamanan pada sistem Analisis ini bertujuan untuk melakukan identifikasi perangkat yang saat ini berjalan, supaya saat implementasi *backup data* tidak terjadi gangguan atau terhentinya operasional perusahaan PT. Global Media Utama Teknologi, lalu mengetahui *data* apa saja yang akan dilakukan *backup*, selanjutnya menambah keamanan pada infrastruktur *backup.*

3.1.1. Topologi Saat ini

Dari hasil analisa sebelumnya, maka didapatkan topologi saat ini seperti gambar 3 di bawah ini.



Gambar 3. Topologi Saat Ini

3.1.2. Kebutuhan *Backup Data*

Pada *tabel* di bawah menjelaskan tabel 1 dari kebutuhan *backup*.

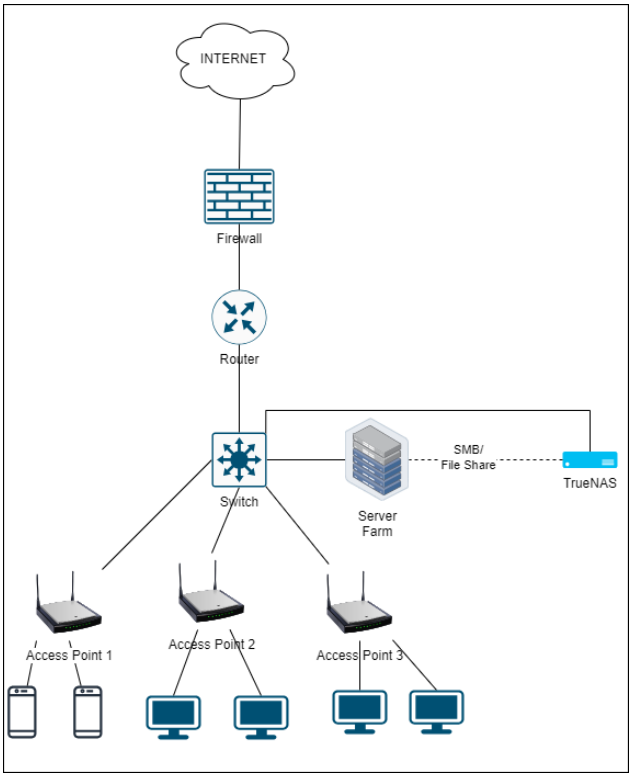
Tabel 1. Kebutuhan *backup*

No	*File*/Folder/*Host* VM	Ukuran Total (GB)
1	D:/GUT2	10 GB
2	D:/MCI	8GB
3	D:/SDM	2GB
4	Active-Directory	512GB
5	Email-Server	256GB
6	GUT-APP-CRM	200GB
7	GUT-APP-CRM-OLD	512GB
8	GUT-WEB-Ecommerce	256GB

3.2. Perancangan Sistem

Perancangan sistem adalah langkah dalam pengembangan sistem yang melibatkan definisi arsitektur, komponen, modul, antar muka, dan data. Fokusnya adalah implementasi kebutuhan dan spesifikasi yang telah diidentifikasi pada tahap sebelumnya. Pada tahap ini, penulis akan merancang topologi implementasi, dan interaksi antara *management server*, *agent server* yang di mana sangat dibutuhkan agar sistem *backup* aplikasi *Acronis Cyber Protect* dapat berjalan sesuai dengan kebutuhan, dan strategi *backup* agar mencegah terjadinya *I/O WAIT* yang tinggi saat melakukan *backup*.

3.2.1. Topologi Implementasi

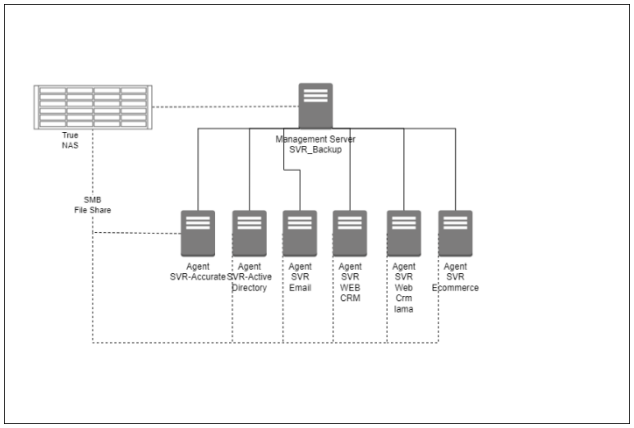


Gambar 4. Topologi saat ini

Gambar 4 di atas adalah menggambarkan topologi yang akan diimplementasikan, dengan melakukan pemisah TrueNAS di luar server *farm* dan dilakukan *filtering* terhadap koneksi yang terhubung ke NAS. Selanjutnya untuk server *Acronis Cyber Protect* ada di dalam server *farm*. Dengan menerapkan pemisahan antara Server *farm* dengan TrueNAS bisa melindungi dari kehilangan *backup*.

3.2.2. *Management* dan *Agent Server*

Acronis Cyber Protect memerlukan *management server* sebagai kontrol terhadap *server-server* yang menjalankan *Acronis Cyber Protect Agent*. Selanjutnya Agent akan terhubung dengan *server Acronis Cyber Protect managemen server* lalu melakukan koneksi ke *TrueNAS*. Berikut pada gambar 5 tentang *management* server.



Gambar 5. *Management Server*

3.2.3. Strategi *Backup*

Untuk mencegah terjadinya penumpukan *IOPS (Input Output Per Second)* karena keterbatasan perangkat *Hard Disk*. Diperlkukan adanya strategi agar *backup* tidak terlalu lama dan *backup* tetap konsisten. Berikut untuk daftar tabel 2 yaitu strategi *backup*.

Tabel 2. Strategi *backup*

No	*File*/Folder/*Host* VM	Ukuran Total (GB)	Tipe *Backup* dan Jadwal *Backup*		
			Incremental backup	*Diffrential backup*	*Full backup*
1	D:/GUT2	10 GB	Setiap hari dalam 1 Minggu di jam 19:00		1 Bulan sekali di tanggal 29 setiap bulan
2	D:/MCI	8GB	Setiap hari dalam 1 Minggu di jam 21:00		1 Bulan sekali di tanggal 29 setiap bulan
3	D:/SDM	2GB	Setiap hari dalam 1 Minggu di jam 22:30		1 Bulan sekali di tanggal 29 setiap bulan
4	Active-Directory	512GB			2 Bulan sekali di tanggal 10 setiap bulan
5	Email-Server	256GB	Seminggu 1x pada hari selasa di jam 20:00		1 Bulan sekali di tanggal 15 setiap bulan
6	GUT-APP-CRM	200GB	Seminggu 1x pada hari kamis di jam 20:00		2 Bulan sekali di tanggal 10 setiap bulan
7	GUT-APP-CRM-OLD	512GB			1x setiap tahun
8	GUT-WEB-Ecommerce	256GB	Seminggu 2x pada hari sabtu dan minggu di jam 22:00		1 Bulan sekali di tanggal 20 setiap bulan

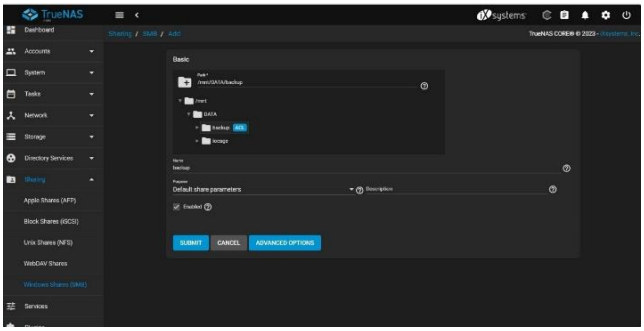
3.3. Implementasi

Pada tahap ini pembahasan mengenai implementasi dalam membangun rancangan infrastruktur *backup data*.

3.3.1 Implementasi TrueNAS

Untuk menampung hasil *backup* maka diperlukan untuk membuat *folder* hasil *backup* di dalam TrueNAS dan selanjutnya dilakukan konfigurasi untuk *services SMB (server Message Block)* agar perangkat-perangkat yang akan dilakukan *backup* terhadap *file* atau *folder* bisa terhubung tanpa ada kendala.

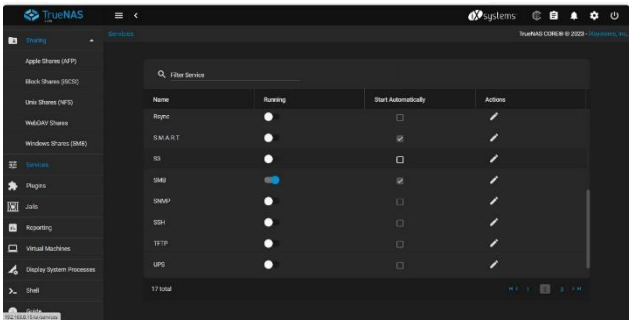
1. Membuat *folder share*



Gambar 6. Membuat *Folder Share*

Folder share pada gambar 6 di atas yang sudah dibuat bisa digunakan untuk menaruh hasil *backup* yang dimana nantinya *server-server agent* dari aplikasi *Acronis Cyber Protect* akan terhubung langsung ke TrueNAS dengan menggunakan protokol SMB *(Server Message Block).*

2. Mengaktifkan *Service* SMB *(Server Message Block)*



Gambar 7. Mengaktifkan *Server SMB (Server Message Block)*

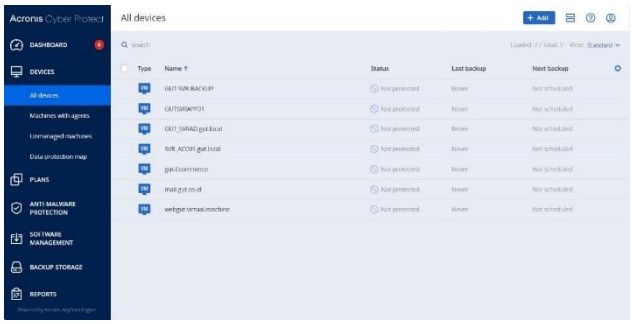
Gambar 7 di atas menjelaskan tentang SMB *(Server Message Block)* diperlukan agar *folder share* yang sudah buat bisa terhubung dan bertukar *data* antara *server-server backup agent Acronis Cyber Protect* dan juga bisa terhubung dengan *client-client* yang akan menggunakan *folder share* nanti kedepannya dengan menggunakan *protocol* dari *SMB (Server Message Block)*.

3.3.2. Implementasi *Acronis Cyber Protect*

Acronis Cyber Protect diperlukan untuk menjalankan *backup* terhadap *file/folder* yang akan dilakukan *backup,* Untuk bisa menjalankan aplikasi *Acronis Cyber Protect* perlu memasang aplikasi *Acronis Cyber Protect* pada *Server* yang akan dijadikan *management* dari aplikasi *Acronis Cyber Protect* dan diperlukan memasangkan *Agent Acronis Cyber protect* pada *server* yang akan dilakukan *backup.*

1. Menambahkan *Server* yang akan melakukan *Backup*

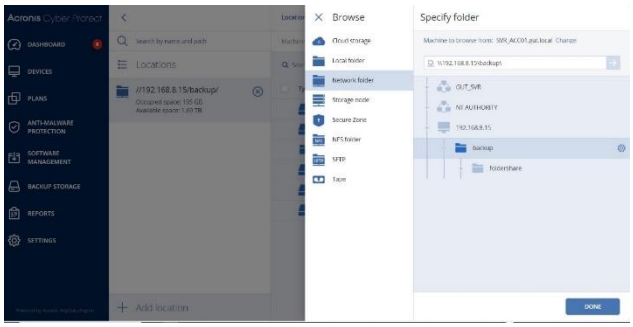
Pada gambar 8 di bawah akan menambahkan *server* yang akan melakukan *backup*



Gambar 8. Menambahkan *Server* yang akan melakukan *Backup*

Untuk bisa melakukan *backup* terhadap *data* maka diperlukan aplikasi *Agent* dari aplikasi *Acronis Cyber Protect* yang terpasang pada *server* yang akan di-*backup* di sini sudah terdapat *server* yang sudah terpasang aplikasi *Agent* dari aplikasi *Acronis Cyber Protect.*

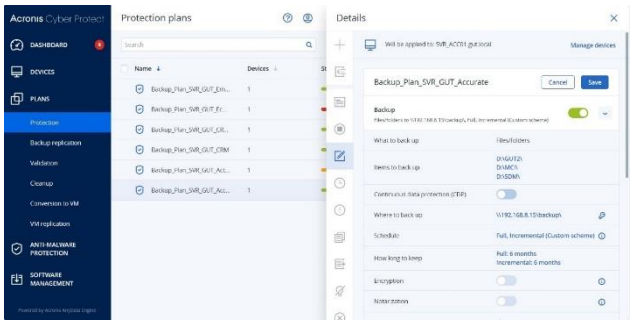
2. Menentukan Lokasi Tempat Penyimpanan Hasil *Backup*



Gambar 9. Menentukan Lokasi Tempat Penyimpanan Hasil *Backup*

Pada gambar 9 di atas digunakan untuk menyimpan hasil *backup*, diperlukan adanya *koneksi* dari *Agent* yang terpasang pada *server* ke TrueNAS dengan koneksi SMB *(Server Message Block)* selanjutnya menentukan di mana *folder* sebagai tempat menyimpan hasil *backup* yang sudah dijalankan secara otomatis.

3. Membuat Jadwal *Backup Server Accurate*

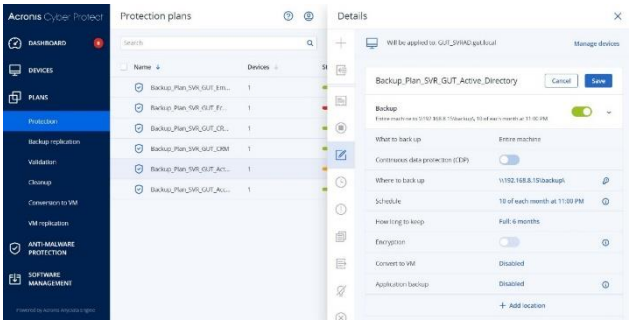


Gambar 10. Membuat Jadwal *Backup Server Accurate*

Pada gambar 10 ini *backup* bisa dilakukan, *backup* secara otomatis dan terjadwal di perlukan adanya sebuah *Plans*

pada *agent acronis* yang terpasang agar *Agent* dapat mengenali jadwal *backup* dan tujuan hasil *backup* yang sudah dilakukan. Maka selanjutnya, pembuatan jadwal *backup* dilakukan disisi *Acronis Cyber Protect Management Server*. Pada *plans* untuk *server accurate* dilakukan setiap hari dengan metode *incrementall backup*, selanjutnya *backup* dengan metode *full backup* dilakukan 1 bulan sekali pada tanggal 29 di setiap bulannya.

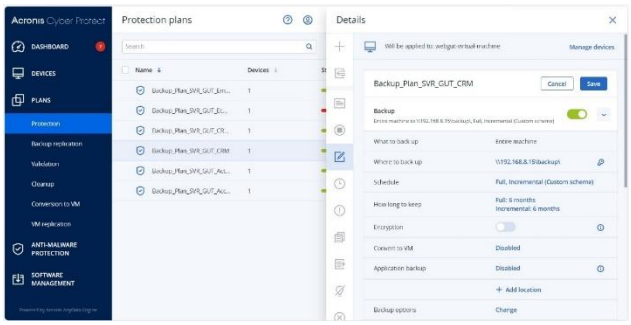
4. Membuat Jadwal *Backup Server Active Directory*



Gambar 11. Membuat Jadwal *Backup Server Active Directory*

Selanjutnya pada gambar 11 *server Active Directory* diperlukan adanya *backup* untuk mencegah terjadinya kehilangan dengan metode *full backup* pada tanggal 10 di setiap bulannya, dan *backup* dijadwalkan berjalan di jam 23:00 WIB(Waktu Indonesia barat).

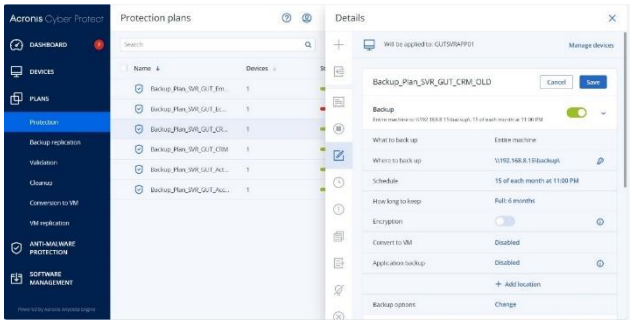
5. Membuat Jadwal *Backup Server* GUT CRM



Gambar 12. Membuat Jadwal *Backup Server* GUT CRM

Selanjutnya pada gambar 12 *server* GUT CRM *(Customer Relationship Management)* sangat penting karena di dalam *server* tersebut terdapat data mengenai penjualan, pembelian, pelanggan, dan Jumlah transaksi, dengan pentingnya data tersebut. Perusahaan menginginkan *server* GUT CRM juga dilakukan *backup*. Maka dibuatkan *Plans* untuk *server* GUT CRM dengan metode *incrementall backup* dengan jadwal 1 minggu satu kali di jam 20:00 WIB, dan untuk metode *full backup* dilakukan pada tanggal 14 di setiap bulannya.

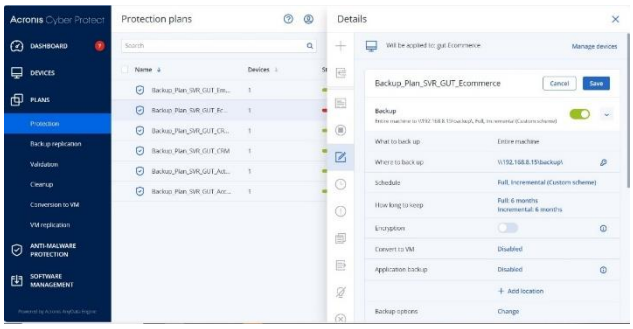
6. Membuat jadwal *backup server* GUT CRM OLD



Gambar 13. Membuat Jadwal *Backup Server* GUT CRM OLD

Pada gambar 13 membuat jadwal ketika Perusahaan juga ingin adanya *backup* terhadap *server* CRM lama, karena masih banyak sekali data penting yang tidak bisa dipindahkan ke *server CRM* baru. *Plans* dengan metode *full backup* 1 tahun 1 kali dan dijadwalkan setiap tanggal 15 Januari dijam 23:00 WIB.

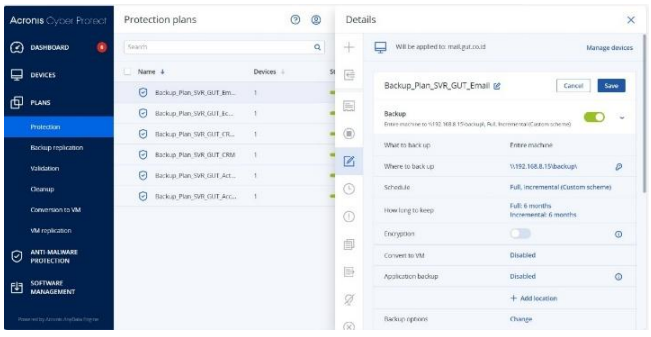
7. Membuat Jadwal *Backup Server* GUT *Ecommerce*



Gambar 14. Membuat Jadwal *Backup Server* GUT *Ecommerce*

Pada gambar 14 ini pembuatan *plans backup* juga dilakukan pada *server* GUT *Ecommerce* dengan metode *incrementall backup* 2 kali pada hari Sabtu dan Minggu setiap minggunya pada jam 22:00, Selanjutnya metode *full backup* dilakukan 1kali sebulan pada setiap tanggal 20.

8. Membuat Jadwal *Backup Server Email*



Gambar 15. Membuat Jadwal *Backup Server Email*

Gambar 15 membuat jadwal *backup*, *Email* adalah surat elektronik yang sangat diperlukan untuk melakukan surat-menyurat pada setiap perusahaan. Dengan sangat pentingnya *server email* perusahaan juga ingin dilakukan adanya *backup*. Metode *backup* dilakukan dengan metode *incrementall backup* dengan jadwal satu minggu satu kali pada hari Selasa pada jam 20:00, dan satu bulan sekali pada tanggal 14 setiap bulannya.

3.4 Evaluasi dan Pengujian

Pada tahap ini dilakukannya evaluasi dan terhadap implementasi rancangan infrastruktur *backup* PT. Global Media Utama Teknologi. Tujuan dari evaluasi ini adalah untuk menilai kesesuaian implementasi sesuai dengan kebutuhan yang telah ditentukan. Untuk melakukan evaluasi, penulis menggunakan metode pengujian *black box testing*, *User Acceptance Testing* (UAT), uji *backup*, *uji restore*.

3.4.1. Hasil *black box testing*

Pada tabel 3 di bawah ini, rincian dari hasil *black box* testing.

Tabel 3. Hasil *Black box Testing*

No	Pengujian	Ekspektasi	Hasil
1	NAS *(Network Attached Storage)* berfungsi dengan baik sesuai harapan	NAS dapat berfungsi dengan baik	Berhasil
2	*Harddisk* di pasang ke dalam NAS	*Harddisk* terdeteksi oleh NAS	Berhasil
3	Membuat partisi di dalam NAS	Partisi dapat di buat	Berhasil
4	Melakukan konfigurasi *ip Address* untuk perangkat *NAS*	*IP Address* berhasil di buat	Berhasil
5	Membuat *Folder sharing* untuk tempat penampung *backup*	Folder *sharing* berhasil di buat	Berhasil
6	Menghidupkan servis SMB*(Server Massage Block)*	*Service* SMB dapat di hidupkan	Berhasil
7	Membuat *User* untuk *Folder Sharing* hasil *backup*	*User* berhasil di buat	Berhasil
8	Melakukan instalasi aplikasi *Acronis Cyber Protect* pada *server backup*	Aplikasi berhasil di pasang pada *server backup*	Berhasil
9	Pengguna dapat masuk kedalam aplikasi *Acronis Cyber Protect*	Menampilkan halaman *dashboard*	Berhasil
10	Melakukan penambahan *Folder Sharing Backup* NAS ke dalam aplikasi *Acronis Cyber Protect*	*Folder sharing backup* berhasil ditambahkan	Berhasil
11	Membuat p*olicy backup data full* yaitu setiap hari minggu jam 12:00 malam dan menyalakan a*ntivirus* untuk *policy*	Policy *backup Berhasil di buat*	Berhasil
12	*Administrator* aplikasi *Acronis Cyber Protect* dapat menambahkan pengguna baru	Pengguna dapat di tambahkan	Berhasil
13	*Administrator aplikasi Acronis Cyber Protect* dapat menghapus *Policy backup* yang sudah di buat	*Policy backup* yang sudah di buat dapat di hapus	Berhasil
14	*Administrator* aplikasi *Acronis Cyber Protect* dapat mengganti jadwal *backup* yang sudah di buat	*Policy backup* dapat di ganti jadwalnya	Berhasil
15	*Administrator* aplikasi *Acronis Cyber Protect* dapat merubah tipe *backup* menjadi *incremental backup* atau *diffrential backup*	*Policy backup* dapat di ganti tipe *backup* nya	Berhasil

3.4.2 Hasil *UAT (User Acceptance Testing)*

Pada tabel 4 berikut berisi informasi data dari hasil UAT (*User Acceptance Testing*).

Tabel 4. Hasil UAT (*User Acceptance Testing)*

No	Pengujian	Ekspektasi	Catatan
1	Pengguna dapat masuk ke dalam NAS	Sesuai	-
2	Pengguna dapat membuat folder di dalam NAS	Sesuai	-
3	Aplikasi *backup acronis cyber protect* berhasil di *install* pada *server*	Sesuai	-
4	*Administrator* dapat masuk kedalam aplikasi backup *acronis cyber protect*	Sesuai	-
5	*Administrator* dapat membuat *policy backup*	Sesuai	-
6	*Administrator* dapat melihat *report backup*	Sesuai	-
7	*Administrator* dapat melihat *report virus* yang terdeteksi	Sesuai	-
8	*Administrator* dapat menjeda *backup* yang sedang berlangsung	Sesuai	-
9	*Administrator* dapat melanjutkan *backup* yang terjeda	Sesuai	-
10	*Administrator* dapat melihat *guest agent acronis* yang sedang berjalan	Sesuai	-

3.4.3 Hasil *backup*

Pada tabel 5 di bawah ini menjelaskan data hasil *backup*.

Tabel 5. Hasil *Backup*

No	*Server/Virtual Machine*	Tipe Kompresi	*Byte* Data Yang Di Proses	*Byte* Data Yang Berhasil Di *Backup*	Rasio Kompresi	Waktu Yang Di Perlukan Untuk *Backup*
1	SVR_Accurate	*High*	953 MB	47.6 MB	4.99%	10 Menit
2	SVR_Active_directory	*High*	152 GB	105 GB	69.08%	1 Jam, 25 Menit
3	SVR_GUT_CRM	*High*	27.4 GB	13.1 GB	47.81%	23 Menit
4	SVR_GUT_CRM_OLD	*High*	32.6 GB	11.4 GB	34.97%	48 Menit
5	SVR_GUT_ECOMMERCE	*High*	38.9 GB	13.4 GB	34.45%	35 Menit
6	SVR_GUT_EMAIL	*High*	83.6 GB	26.4 GB	31.55%	1 Jam, 32 Menit

Berdasarkan dari hasil *testing backup data* di atas, dengan dilakukannya *backup* terhadap *server-server* yang sudah ditentukan. Maka didapati rasio kompresi setiap *backup* didapatkan tergantung pada data yang dilakukan *backup*. Kompresi akan sangat berguna untuk menghemat kapasitas ruang penyimpanan. Selanjutnya untuk mendapatkan rasio kompresi adalah dengan menggunakan rumus sebagai berikut: Persentase rasio = (*Byte* yang diproses / *Byte* data yang berhasil di-*backup*) x 100%

3.4.4 Hasil *restore*

Pada tabel 6 berikut dijelaskan hasil dari *restore*.

Tabel 6. Hasil *Restore*

No	*Server/Virtual Machine*	Tipe *Backup*	Jenis *Backup*	*Byte* Data yang Diproses	Waktu yang Diperlukan untuk *Backup*	Status *Restore*
1	SVR_Accurate	*Full*	*File/Folder*	953 MB	10 Menit	Berhasil
2	SVR_Active_directory	*Full*	*Entire Machine*	152 GB	2 Jam, 58 Menit	Berhasil
3	SVR_GUT_CRM	*Full*	*Entire Machine*	27.4 GB	17 Menit	Berhasil
4	SVR_GUT_CRM_OLD	*Full*	*Entire Machine*	32.6 GB	28 Menit	Berhasil
5	SVR_GUT_ECOMMERCE	*Full*	*Entire Machine*	38.9 GB	25 Menit	Berhasil
6	SVR_GUT_EMAIL	*Full*	*Entire Machine*	83.6 GB	1 Jam, 55 Menit	Berhasil

Selanjutnya setelah melakukan *testing backup.* Penulis juga melakukan *testing restore* terhadap *server-server* yang sudah berhasil dilakukan *backup*. Didapati *restore* dari masing-masing *server* berhasil, maka selanjutnya untuk kecepatan *restore* bergantung pada *Input Output Per Second* (IOPS) dari masing-masing tipe penyimpanan hasil *backup,* dan media yang digunakan untuk melakukan *transfer* data.

4. KESIMPULAN

Dalam upaya mencegah terjadinya kehilangan data terutama pada PT. Global Media Utama Teknologi. Penelitian ini berhasil merancang dan mengimplementasikan sistem *backup* menggunakan aplikasi *Acronis Cyber Protect.* Tahap awal dalam proses membuat rancangan infrastruktur *backup data* di PT. Global Media Utama Teknologi, melibatkan proses perumusan masalah melalui studi pendahuluan. Selanjutnya proses analisis sistem dimulai dari topologi saat ini, daftar perangkat, kebutuhan *backup data*, *role account,* pembatasan perangkat, dan perancangan sistem mencakup desain sistem, topologi implementasi, *management server* dan *agent server*, dan strategi *backup.* Kemudian implementasi, dilakukan dengan membangun NAS *(Network Attached Storage)*, konfigurasi NAS *sharing folder*, *server management acronis cyber protect,* konfigurasi *plans* untuk *backup*. Hasil dari *Black Box Testing* didapati pada saat dilakukan testing dapat diambil kesimpulan berhasil tanpa adanya gangguan atau *Error* pada saat testing. Dengan hadirnya rancangan infrastruktur *backup data* di PT. Global Media Utama Teknologi, selain menawarkan solusi *backup* terhadap *data, Virtual Machine* (VM), juga memberikan keuntungan dalam hal keamanan terhadap pemindaian *file* yang terinfeksi oleh *virus*¸ atau *virus* itu sendiri saat proses *backup*. Maka dari itu dengan adanya aplikasi *Acronis Cyber Protect* diharapkan dapat meningkatkan keamanan *data* pada saat proses *backup.*

Melalui hasil uji akhir dengan *User Acceptance Testing* (UAT), *Backup Testing* dengan rata-rata waktu yang

diperlukan untuk *backup* adalah 48,83 menit, *Restore Testing* memerlukan waktu rata-rata 59 menit. Nilai rata-rata waktu *backup* dan *restore* bisa fluktuatif tergantung dari media penyimpanan hasil *backup*, media transmisinya, dan jumlah data yang dilakukan *backup* dan *restore*. Menunjukkan bahwa implementasi rancangan infrastruktur *backup* pada PT. Global Media Utama Teknologi, berhasil dan memenuhi kebutuhan pengguna. Melihat hasil *UAT, Backup Testing, Restore Testing* yang telah didapatkan dan diuji dapat disimpulkan bahwa implementasi rancangan infrastruktur *backup* pada PT. Global Media Utama Teknologi, membawa dampak positif dalam upaya mencegah terjadinya kehilangan data akibat dari serangan siber ataupun ketidaksengajaan saat operasional perusahaan sedang berlangsung.

DAFTAR PUSTAKA

[1] D. A. Arifah, "Kasus Cybercrime Di Indonesia," *Jurnal Bisnis dan Ekonomi (JBE),* vol. 18, 2011.

[2] S. Muhamad Danuri, "Trend Cyber Crime dan Teknologi Informasi di Indonesia," *INFOKAM,* 2017.

[3] S. Laan, IT Infrastructure Architecture - Infrastructure Building Blocks and Concepts, Sjaak Laan, 2011.

[4] P. W. D. R. Jeanne W. Ross, Enterprise Architecture as Strategy: Creating a Foundation for Business Execution, 2006.

[5] J. Hutahaean, "Konsep Sistem informasi," dalam *Konsep Sistem informasi / oleh Jeperson Hutahaean*, Yogyakarta, 2014.

[6] Wikipedia, "Rekam Cadang," [Online]. Available: https://id.wikipedia.org/wiki/Rekam_cadang#cite_note-1. [Diakses 12 Maret 2024].

[7] J. Andry, "Pengembangan Aplikasi Backup dan Restore secara Automatisasi menggunakan SDLC untuk Mencegah Bencana," *Journal Muara sains Teknologi, Kedokteran, dan ilmu kesehatan,* vol. 1, April 2017.

[8] W. C. Preston, Backup & Recovery: Inexpensive Backup Solutions for Open Systems, 2007.

[9] Acronis, "Informasi dan sejarah perusahaan acronis," [Online]. Available: https://www.acronis.com/id-id/company/. [Diakses 12 Maret 2024].

[10] Acronis, "Acronis Cyber Protect," [Online]. Available: https://www.acronis.com/id-id/products/cyber-protect. [Diakses 12 maret 2024].

[11] PT. Global Media Utama Teknologi, "About Us," [Online]. Available: http://globaltekno.com. [Diakses 12 maret 2024].

[12] B. Hartono, "Ransomware: Memahami Ancaman Keamanan Digital," *Bincang Sains dan teknologi,* vol. 2, Agustus 2022.

[13] S. W. H. Prastyo, "Pengujian Sistem Informasi Lembaga Donasi Berbasis Web Menggunakan Metode Black Box Testingdan Teknik Equivalence Partitions," *OKTAL : Jurnal Ilmu Komputer dan Science,* vol. 2, 2023.

[14] W. I. Fahrullah, "Analisis Blackbox Testing dan User Acceptance Testing terhadap Sistem Informasi Solusimedsosku," *Jurnal Teknosains Kodepena,* vol. 04, 2023.

[15] B. Gonzalez, "What Is a NAS (Network Attached Storage) Device?," 2 12 2020. [Online]. Available: https://www.lifewire.com/what-is-a-nas-1847428. [Diakses 27 maret 2024].

[16] Truenas, "Truenas," [Online]. Available: https://www.truenas.com/faq/. [Diakses 3 maret 2024].

[17] Microsoft, "Microsoft SMB Protocol and CIFS Protocol Overview," 1 Agustus 2021. [Online]. Available: https://learn.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview?redirectedfrom=MSDN. [Diakses 2024 maret 2024].