SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

RANCANGAN INFRASTRUKTUR BACKUP DATA DI PT. GLOBAL MEDIA UTAMA TEKNOLOGI

TUGAS AKHIR

IQBAL NAVELIANO

0110120111

PROGRAM STUDI SISTEM INFORMASI

STT TERPADU NURUL FIKRI

Juni 2024

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

RANCANGAN INFRASTRUKTUR BACKUP DATA DI PT. GLOBAL MEDIA UTAMA TEKNOLOGI

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

IQBAL NAVELIANO
0110120111

PROGRAM STUDI SISTEM INFORMASI
STT TERPADU NURUL FIKRI
Juni 2024

HALAMAN PERNYATAAN ORISINALITAS

Skripsi/Tugas Akhir ini adalah hasil karya penulis, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama :Iqbal Naveliano

NIM : 0110120111

Jakarta, 1 Agustus 2024

Tanda Tangan

Iqbal Naveliano

HALAMAN PENGESAHAN

Skripsi/Tugas Akhir ini diajukan oleh :

Nama : IQBAL NAVELIANO

NIM : 0110120111

Program Studi : Sistem Informasi

Judul Skripsi : RANCANGAN INFRASTRUKTUR BACKUP DATA DI PT. GLOBAL MEDIA UTAMA TEKNOLOGI

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Sistem Informasi, Sekolah Tinggi Teknologi Terpadu Nurul Fikri

DEWAN PENGUJI

Pembimbing	Penguji
1/8/24	
(Suhendi, S.T., M.M.S.I.)	(Efrizal Zaida, S.Kom., M.M., M.Kom.)

Ditetapkan di : Jakarta

Tanggal : 27 Juli 2024

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan skripsi/Tugas Akhir ini. Penulisan skripsi/Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana komputer Program Studi Sistem informasi pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi/tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT.
2. Orang tua dan semua anggota keluarga yang telah memberikan dorongan baik secara moril maupun materil dalam penyelesaian tugas ini.
3. Bapak Drs. Rusmanto, M.M., selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Ibu S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
5. Bapak Suhendi, S.T, M.M.S.I., selaku Dosen Pembimbing Akademik yang telah membimbing penulis selama berkuliah di Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Bapak Suhendi, S.T, M.M.S.I., selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
7. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
8. PT. Global Media Utama Teknologi Manajer Hadi Surya Jaya beserta karyawan yang telah meluangkan waktunya untuk memberikan data yang diperlukan bagi penulisan ilmiah ini.

Dalam penulisan ilmiah ini tentu saja masih banyak terdapat kekurangan-kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan yang penulis miliki. Walaupun demikian, penulis telah berusaha menyelesaikan penulisan

ilmiah ini sebaik mungkin. Oleh karena itu apabila terdapat kekurangan di dalam penulisan ilmiah ini, dengan rendah hati penulis menerima kritik dan saran dari pembaca.

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 19 Juni 2024

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini:

Nama : Iqbal Naveliano
NIM : 0110120111
Program Studi : Sistem Informasi
Jenis karya : Tugas Akhir

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STT-NF **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty - Free Right*)** atas karya ilmiah saya yang berjudul :

Rancangan Infrastruktur Backup PT. Global Media Utama Teknologi

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini STT-NF berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 5 Agustus 2024

Yang Menyatakan

(Iqbal Naveliano)

ABSTRAK

(300 kata)

Nama : IQBAL NAVELIANO

NIM : 0110120111

Program Studi : Sistem Informasi

Judul : RANCANGAN INFRASTRUKTUR BACKUP DATA DI PT. GLOBAL MEDIA UTAMA TEKNOLOGI

Dengan maraknya serangan siber yang menimpa ruang siber Indonesia beberapa waktu ini, mengakibatkannya kehilangan *data* suatu perusahaan, terlebih serangan siber saat ini sangat membahayakan *data* perusahaan. Pada tahun 2022 perusahaan PT. Global Media Utama teknologi mengalami serang siber ransomware yang mengakibatkan kehilangan *data* dan membuat kerugian pada perusahaan. Maka dari kejadian tersebut diperlukannya solusi untuk mencegah terjadinya kehilangan *data* akibat dari serangan siber atau ketidak sengajaan dalam operasional perusahaan. Dengan dilakukannya implementasi rancangan infrastruktur *backup data* di PT. Global Media Utama Teknologi, dengan menggunakan beberapa teknologi seperti *Network Attached Storage (NAS)* dan aplikasi *backup* dari perushaaan *acronis* bernama *acronis cyber protect.* Selanjutnya melalui uji akhir dengan menggunakan *black box testing, User Acceptence Testing (UAT), backup testing,* dan *restore testing* menunjukkan rancangan infrastruktur *backup* di PT. Global Media Utama Teknologi berjalan sesuai dengan keinginan pengguna.

Kata kunci :backup, NAS, restore, ransomware

ABSTRACT

Name : Iqbal Naveliano

NIM : 0110120111

Study Program : Sistem Informasi

Title : Rancangan infrastruktur backup PT. Global Media Utama Teknologi

With the rise of cyber attacks affecting Indonesia's cyberspace recently, resulting in data loss for companies, cyber attacks have become highly dangerous to company data. In 2022, PT. Global Media Utama Teknologi experienced a ransomware cyber attack that caused data loss and financial damage to the company. Due to this incident, a solution is needed to prevent data loss due to cyber attacks or operational accidents within the company. Therefore, PT. Global Media Utama Teknologi implemented a backup infrastructure design using technologies such as Network Attached Storage (NAS) and backup applications from Acronis called Acronis Cyber Protect. Subsequently, through final testing using black box testing, User Acceptance Testing (UAT), backup testing, and restore testing, it was shown that the backup infrastructure design at PT. Global Media Utama Teknologi met user requirements.

Key words : *backup, NAS, restore, ransomware*

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS 3
HALAMAN PENGESAHAN 4
KATA PENGANTAR 5
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI 7
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS 7
ABSTRAK 8
ABSTRACT 9
DAFTAR ISI 10
DAFTAR GAMBAR 14
DAFTAR TABEL 15
BAB I 16
PENDAHULUAN 16
1.1 Latar belakang 16
1.2 Rumusan Masalah 18
1.3 Tujuan dan Manfaat Penelitian 18
1.4 Batasan Masalah 19
1.5 Sistematika Penulisan 19
BAB II KAJIAN LITERATUR 21
2.1 Landasan Teori 21
2.1.1 Rancangan infrastuktur teknologi informasi 21
2.1.2 Infrastruktur Jaringan 21
2.1.3 Sistem informasi 21
2.1.4 *Backup* 22

2.1.5 Metodologi *backup* 22
2.1.6 *Incremental backup* 22
2.1.7 *Differential backup* 22
2.1.8 *Full Backup* 22
2.1.9 *Acronis Cyber Protect* 23
2.1.9 PT. Global Media Utama Teknologi 23
2.1.10 Topologi 23
2.1.11 *Ransomware* 23
2.1.12 *Anti-Virus* 24
2.1.13 *Malware* 24
2.1.14 *Black Box Testing* 24
2.1.15 *UAT(User Acceptance Testing)* 24
2.1.16 *NAS(Network Attached Storage)* 24
2.1.17 *Truenas* 24
2.1.18 *SMB (Server Message Block)* 25
2.2 Penelitian terkait 25
BAB III METODOLOGI PENELITIAN 27
3.1 Tahapan Penelitian 27
3.1.1 identifikasi Masalah 28
3.1.2 Studi Literatur 28
3.1.3 Analisis Kebutuhan 28
3.1.4 Perancangan Topologi 28
3.1.5 Implementasi 29
3.1.7 Pengujian 31
3.1.8 Evaluasi 31

3.2 Rancangan Penelitian 32
3.2.1 Jenis Penelitian 32
3.2.2 Metode Analisis 32
3.2.3 Metode Pengumpulan Data 32
3.2.4 Lingkungan Pengembangan 36
3.2.5 Waktu Penelitian (*Gantt Chart*) 37
3.2.6 Metode Implementasi dan Evaluasi 37
BAB IV IMPLEMENTASI DAN EVALUASI 38
4.1. Analisis Sistem 38
4.1.1 Topologi saat ini 39
4.1.2 Daftar perangkat 39
4.1.3 Kebutuhan *Backup Data* 40
4.1.4 *Role Account* 40
4.1.5 Pembatasan perangkat 41
4.2 Perancangan sistem 42
4.2.1 Desain Sistem 43
4.3 Implementasi 47
4.3.1 Implementasi *TrueNAS* 47
4.3.2 Implementasi *Acronis Cyber Protect* 49
4.4 Evaluasi dan Pengujian 55
4.4.1 Hasil Black Box Testing 55
4.4.2 Hasil UAT 58
4.4.3 Hasil *Backup* 59
4.4.4 Hasil Restore 60
BAB V KESIMPULAN DAN SARAN 61

5.1 Kesimpulan 61
5.2 Saran 62
DAFTAR REFERENSI 63
LAMPIRAN 66

DAFTAR GAMBAR

Gambar 1 Tahapan Penilitian 27
Gambar 2 Tahapan Implementasi 29
Gambar 3 Waktu Penilitian 37
Gambar 4 1 Topologi saat ini 39
Gambar 4 2 Topologi Implementasi 43
Gambar 4 3 Acronis Management Server & Acronis Agent Server 44
Gambar 4 4 Strategi backup 45
Gambar 4 5 Membuat folder share 47
Gambar 4 6 Mengaktifkan service SMB (Server Message Block) 48
Gambar 4 7 menambahkan pengguna acronis cyber protect 49
Gambar 4 8 Menambahkan server yang akan melakukan backup 50
Gambar 4 9 Menentukan lokasi tempat penyimpanan hasil backup 50
Gambar 4 10 membuat jadwal backup server accurate 51
Gambar 4 11 Membuat jadwal backup server active directory 52
Gambar 4 12 Membuat jadwal backup server GUT CRM 52
Gambar 4 13 Membuat jadwal backup server GUT CRM OLD 53
Gambar 4 14 Membuat jadwal backup server GUT Ecommerce 54
Gambar 4 15 Membuat jadwal backup server Email 54

DAFTAR TABEL

Tabel 1. Penelitian Terkait 25
Tabel 2 1 Black Box Testing 33
Tabel 3 1 User Acceptance Test 35
Table 4 1 Daftar perangkat 39
Table 4 2 Kebutuhan backup data 40
Table 4 3 Role Account 40
Table 4 4 Pembatasan perangkat 41
Table 4 5 Hasil black box testing 55
Table 4 6 Hasil UAT 58
Table 4 7 Hasil Backup 59
Table 4 8 Hasil Restore 60

BAB I
PENDAHULUAN

1.1 Latar belakang

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, eeducation dan e-retailing*. Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. [1]

Seiring dengan berkembangnya teknologi informasi dan komunikasi, sistem informasi sangatlah penting bagi operasional bisnis. Orang mengandalkan sistem informasi untuk berkomunikasi melalui berbagai perangkat fisik (perangkat keras), sistem kontrol dan pemrosesan informasi (perangkat lunak), jaringan, dan infrastruktur data. Oleh karena itu, banyak orang yang menganggap manfaat sistem informasi sangat penting dalam rencana bisnisnya. Sistem informasi dapat mengumpulkan, mengatur dan menyediakan informasi yang membantu manajemen perusahaan untuk mengambil keputusan dan rencana, untuk bekerja dan untuk meningkatkan penjualan barang yang di produksi. [2]

Disatu 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 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. [3]

PT. Global Media Utama Teknologi berdiri pada tahun 2010 dan secara legal terdaftar pada kementerian hukum dan ham, berbadan hukum sebagai perseroan terbatas. PT. Global Media Utama Teknologi perusahaan yang bergerak di bidang jasa dan perdagangan.

PT. Global Media Utama teknologi sendiri belum memilik infrastruktur *Backup* untuk data dan juga *server* yang berjalan saat ini. Saat ini data pada PT. Global Media Utama Teknologi berisiko terjadinya kehilangan data dan terkena serangan siber.

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 dimana 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.*

Diharapkan dengan adanya solusi rancangan infrastruktur *backup* data, data perusahaan PT. Global Media Utama teknologi dapat dilindungi dari serangan *virus, malware, ransomware,* ataupun ancaman kehilangan data secara tidak sengaja maupun disengaja. Dengan dibangunnya rancangan solusi infrastruktur *backup* data diharapkan menjawab tantangan-tantangan di dunia siber tentang keamanan data.

1.2 Rumusan Masalah

Dengan melihat latar belakang yang telah dijabarkan sebelumnya, maka rumusan masalah tugas akhir ini adalah :

1. Bagaimana merancang infrastruktur backup data yang efektif untuk melindungi PT. Global Media Utama Teknologi dari serangan ransomware dan kehilangan data.
2. Bagaimana hasil evaluasi terhadap solusi rancangan infrastruktur *backup* data pada PT. Global Media Utama Teknologi.

1.3 Tujuan dan Manfaat Penelitian

Melalui perumusan masalah yang telah dijabarkan, tujuan penelitian yang teridentifikasi adalah :

1. Membangun sebuah solusi untuk permasalahan yang dihadapi oleh PT. Global Media Utama Teknologi.

2. Untuk mengetahui hasil dan melakukan evaluasi terhadap solusi yang diberikan yaitu rancangan infrastruktur *backup* data

Dengan merinci tujuan penelitian diatas diharapankan dapat memberikan kontribusi positif serta manfaat kepada selurutuh pihak. Manfaat tersebut antara lain :

1. Menjawab tantangan terhadap permasalahan yang dihadapi saat ini tentang keamanan data mengenai kehilangan data yang disebabkan oleh serangan *ransomware, virus,* dan *malware.*

2. Sebagai langkah strategis untuk menjawab tantangan tentang mitigasi risiko terhadap kehilangan data yang disebabkan oleh serang didunia siber.

1.4 Batasan Masalah

Untuk menjaga fokus pada tujuan awal, dan mempermudah peneliti dalam mengumpulkan informasi yang diperlukan, peneliti memberikan beberapa batasan antara lain:

1. Hanya melakukan instalasi Agen Acronis Cyber Protect pada Server yang akan dilakukan backup.
2. Tidak melakukan perubahan konfigurasi jaringan yang sudah berjalan.
3. Tidak bisa melakukan *decrypt* terhadap suatu file yang sudah ter-*encrypt* oleh *ransomware.*
4. Membutuhkan *License* berbayar untuk menjalankan aplikasi *Acronis Cyber Protect.*
5. *Data* yang akan dilakukan *backup* adalah data *Finance, Email, Active Directory, Data CRM,* dan *Data Ecommerce.*

1.5 Sistematika Penulisan

Berikut adalah struktur penulisan atau sistematika penulisan tugas akhir :

BAB I PENDAHULUAN

Bab ini membahas bagian awal yang mencakup latar belakang, rumusan masalah, tujuan yang ingin dicapai, manfaat yang diperoleh, batasan masalah, serta sistematika dari penulisan penelitian.

BAB II KAJIAN LITERATUR

Bab ini membahas mengenai teori-teori yang dianggap relevan dengan penelitian ini, dimana teori-teori tersebut akan menjadi dasar acuan untuk menyelesaikan masalah. Bab ini juga mengulas penelitian sejenis yang berkaitan dengan topik yang sedang dilakukan penelitian.

BAB III METODOLOGI PENELITIAN

Pada bab ini membahas tahapan penelitian, mencakup tahapan yang sudah dilakukan dan akan dilakukan. Selain itu, pada bab ini menjelaskan rancangan penelitian yang melibatkan jenis penelitian, metode analisis dan pengumpulan data, lingkungan pengembangan, serta metode implementasi dan evaluasi yang digunakan dalam penelitian.

BAB IV IMPLEMENTASI DAN EVALUASI

Pada BAB ini memuat penjelasan mengenai analisis sistem, dimulai dari kebutuhan pengguna, topologi infrastruktur *backup* data, dan implementasi rancangan infrastruktur *backup* data. Selanjutnya pada tahapan akhir dilakukan pengujian atau evaluasi terhadap rancangan infrastruktur *backup* data yang sudah diimplementasikan dengan menggunakan *black box testing, dan user acceptance testing.*

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan bagian penutup penelitian yang mencakup kesimpulan sebagai jawaban dari rumusan masalah penelitian, serta saran untuk peneliti yang ingin mengembangkan penelitian serupa kedepannya.

BAB II
KAJIAN LITERATUR

2.1 Landasan Teori

Menjelaskan berbagai teori yang dijadikan acuan, terumasuk Sistem informasi, *backup,* metodologi *backup, incremental backup, differential backup, full backup,* Aplikasi *Acronis Cyber Protect,* PT. Global Media Utama Teknologi, topologi, *ransomware, anti-virus, malware, black box testing, UAT, NAS, TrueNAS, SMB.* Penjelasan ini bertujuan memberikan landasan konseptual yang mendalam untuk mendukung pelaksanaan penelitian dengan lebih rapih dan sesuai dengan standar penulisan yang baku.

2.1.1 Rancangan infrastuktur 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. [4]

2.1.2 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 [5] ancaman eksternal maupun internal.

2.1.3 Sistem informasi

Sistem informasi adalah suatu sistem didalam 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 di butuhkan [6].

2.1.4 *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. [7]

2.1.5 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. [8]

2.1.6 *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. [9]

2.1.7 *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. [9]

2.1.8 *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. [9]

2.1.9 *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. [10]

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]

2.1.9 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. [12]

2.1.10 Topologi

Topologi merupakan cara/konsep tata letak yang menjelaskan bagaimana berbagai komputer dan hardware lainnya dapat membangun jaringan komputer. [13]

2.1.11 *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 didekripsi. [14]

2.1.12 *Anti-Virus*

Antivirus disebut juga sebagai perangkat lunak perlindungan dari serangan *malware*. *Antivirus* juga dapat melakukan deteksi *signature based* dan *heuristic based* pada sistem menggunakan fitur *scanning* yang terdapat pada *software* itu sendiri. [15]

2.1.13 *Malware*

Malware, yaitu suatu software yang di-design untuk merusak sistem komputer tanpa memberitahu pemilik komputer tersebut. [16]

2.1.14 *Black Box Testing*

Pengujian black box adalah proses pengujian perangkat lunak yang membutuhkan pengujian aplikasi tanpa mengetahui kode program atau struktur internal aplikasi. [17]

2.1.15 *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. [18]

2.1.16 *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 computer. [19]

2.1.17 *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.* [20]

2.1.18 *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. [21]

2.2 Penelitian terkait

Penelitian ini terinspirasi oleh sejumlah penelitian sebelumnya dengan fokus penelitian serupa.

Tabel 1 Penelitian Terkait

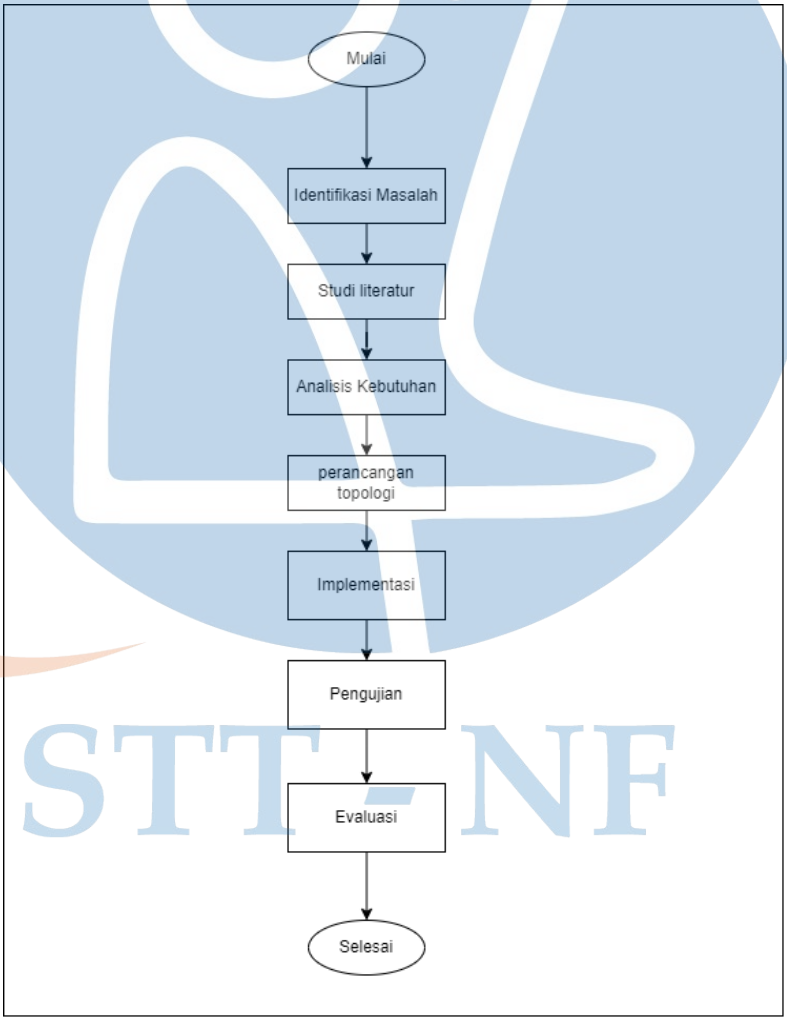
No	Nama dan Tahun	Judul	Topik	Tools	Hasil
1	Ratomi Husnul. Nadhori Uzzin Isbat, 2010	Manajemen *backup data* otomatis pada jaringan menggunakan *Rsync*	Manajemen *backup data*	Sistem operasi *Linux Debian, VMWare Workstation, Rsync*	Solusi penyelamatan data menggunakan aplikasi *Rsync*
2	Faizal Abroni, Arief Prastyo, Sofyan Noor Arief. 2019	Implementasi *disaster recovery plan server system* dengan metode *failover* berbasil linux di politeknik negeri malang	*Disaster Recovery*	*GNU/Linux, VMWare, Veeam.*	Metode *Disaster recovery* menggunakan aplikasi *Veeam*
3	Asep Nurhada, Annafi franz. 2017	Perbandingan pencadangan data menggunakan RSync dan SFTP	Perbandingan pencandangan data	Rsync, SFTP	Perbandingan pencandangan data SFTP dengan Rsync

4	Musa Amin, 2020	*Private cloud storage* sebagai media pencadangan data dan berbagi data secara *real-time*	Menjadikan *private cloud storage* sebagai media pencadangan	*Nextcloud, Linux, Windows*	*Private cloud storage* sebagai media pencadangan
5	Muhammad Iqbal, Lulu Chaerani Munggaran. 2019	*Backup Strategy for IT Disaster Recovery Plan Using Active Data Guard and NetBackup*	*Backup data and IT Disaster recover*	*Active Data Guard, NetBackup*	*Backup Data and IT Disaster Recovery with application Active Data Guard & Netbackup*
6	Shibin Hu,Yiyong Lin,Zhang Qi,Qiang Fu,Jianbiao Chen, 2021	*Research on the Architecture of Cloud Host Autonomous Backup System in a Cloud Data Center*	*Analyze architecture Cloud Host Autonomus Backup System*	*Cloud Compute,SAN*	*Cloud host backup solution*
7	Jason E. Thomas & Gordon C. Galligher, 2018	*Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware*	*Evaluation backup system to combat ransomware*	*Microsoft Securtiy Essentials, Nortel Antivirus*	*Evalation backup system to combat and prevent ransomware*

BAB III
METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

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



Gambar 1 Tahapan Penilitian

3.1.1 identifikasi Masalah

Pada saat ini PT. Global Media Utama Teknologi belum memiliki sebuah infrastruktur *Backup* yang bisa menunjang operasional perushaan. Dimana sangat rentan sekali terjadinya kehilangan data perusahaan yang akan berdampak pada operasioanal perushaan. Berdasarkan permasalah tersebut penulis menganalisa kebutuhan untuk membangun infrastruktur *Backup* yang memungkinkan *Backup* PT. Global Media Utama Teknologi bisa berjalan secara otomatis dan terjadwal serta meminimalisir terjadinya kehilangan data.

3.1.2 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.

3.1.3 Analisis Kebutuhan

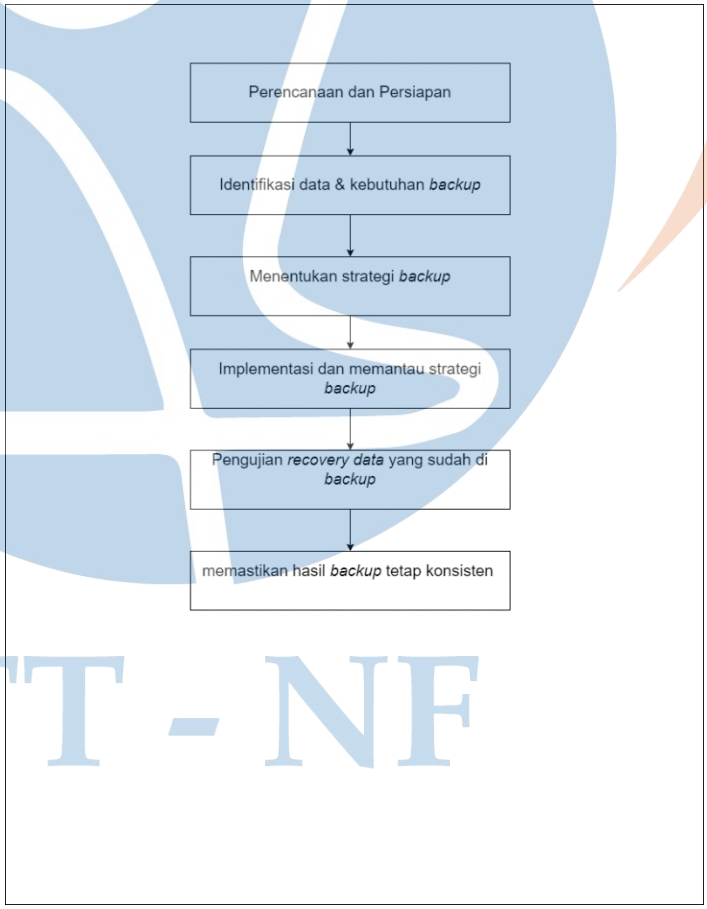
Pada tahapan ini penulis melakukan analisa dari masalah-masalah yang sudah di temukan dan diidentifikasi, sehingga penulis mendapatkan apa saja yang dibutuhkan untuk melakukan perancangan infrastruktur *backup data* di PT. Global Media Utama Teknologi, yang kemudian akan di implementasikan menjadi sebuah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

3.1.4 Perancangan Topologi

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

3.1.5 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 sebagai berikut.



Gambar 2 Tahapan Implementasi

Rancangan *backup* penulis terdiri dari beberapa proses diantaranya:

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* & 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.*

3.1.7 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.

3.1.8 Evaluasi

Pada Tahapan ini penulis melakukan evalusasi 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 infrastuktur *Backup* di PT. Global Media Utama Teknologi.

3.2 Rancangan Penelitian

Penyusunan rancangan penelitian dilakukan untuk menjelaskan rencana menyeluruh dari penelitian, antara lainnya :

3.2.1 Jenis Penelitian

Penelitian ini merupakan penelitian dengan dengan menggunakan penelitian implementasi. Yang Dimana hasil dari penelitian ini akan diimplementasikan langsung pada tempat penelitian. Data yang di peroleh dari observasi, studi Pustaka, dan studi kasus yang penulis pernah lakukan.

3.2.2 Metode Analisis

Metode analisis yang di lakukan 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*.

3.2.3 Metode Pengumpulan Data

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.

Pengujian *Black box testing* dilakukan dengan fokus pada pengetesan spesifik fungsionalitas dari rancangan infrastruktur *backup data* pada PT. Global Media Utama Teknologi :

Tabel 2 1 Black Box Testing

NO	Pengujian	Ekspetasi	Hasil
1	*NAS(Network Attached Storage) berfungsi dengan baik sesuai harapan*	*NAS* dapat berfungsi dengan baik	Berhasil atau Tidak
2	*Harddisk* di pasang kedalam nas	*Harddisk* terdeteksi oleh *NAS*	Berhasil atau Tidak
3	Membuat partisi di dalam *NAS*	Partisi dapat di buat	Berhasil atau Tidak
4	Melakukan konfigurasi *ip Address* untuk perangkat *NAS*	*IP Address* berhasil di buat	Berhasil atau Tidak
5	Membuat *Folder sharing* untuk tempat penampung *backup*	Folder sharing berhasil di buat	Berhasil atau Tidak
6	Menghidupkan servis *SMB(Server Massage Block)*	Service *SMB* dapat di hidupkan	Berhasil atau Tidak
7	Membuat *User* untuk *Folder Sharing* hasil *backup*	*User berhasil di buat*	Berhasil atau Tidak

8	Melakukan instalasi aplikasi *Acronis Cyber Protect* pada *server backup*	Aplikasi berhasil di pasang pada *server backup*	Berhasil atau Tidak
9	Pengguna dapat masuk kedalam aplikasi *Acronis Cyber Protect*	Menampilkan halaman *dashboard*	Berhasil atau Tidak
10	Melakukan penambahan *Folder Sharing Backup NAS* kedalam aplikasi *Acronis Cyber Protect*	*Folder sharing backup* berhasil di tambahkan	Berhasil atau Tidak
11	Membuat p*olicy backup* untuk data yang akan dilakukan *backup* dan menyalakan a*ntivirus* untuk *policy*	Policy *backup Berhasil di buat*	Berhasil atau Tidak
12	*Administrator* aplikasi *Acronis Cyber Protect* dapat menambahkan pengguna baru	Pengguna dapat di tambahkan	Berhasil atau Tidak
13	*Administrator aplikasi Acronis Cyber Protect* dapat menghapus *Policy backup* yang sudah di buat	*Policy backup* yang sudah di buat dapat di hapus	Berhasil atau Tidak
14	*Administrator* aplikasi *Acronis Cyber Protect* dapat mengganti jadwal *backup* yang sudah di buat	*Policy backup* dapat di ganti jadwalnya	Berhasil atau Tidak
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 atau Tidak
16	*Administrator* aplikasi *Acronis Cyber Protect* dapat melihat *report* mengenai *backup*	*Report backup* dapat di tampikan	Berhasil atau Tidak

17	*Administrator* aplikasi *Acronis Cyber Protect* dapat melihat *virus* atau *malware* yang terdeteksi	*Virus* dan *malware* terdeteksi	Berhasil atau Tidak
18	*Administrator* aplikasi *Acronis Cyber Protect* dapat melihat *report virus/malware* yang terdeteksi selama prose *backup*	*Report virus/malware* dapat di tampikan	Berhasil atau Tidak
19	*Administrator* aplikasi *Acronis Cyber Protect* dapat melihat *vulnerability* atau celah terhadap *server*	*Vulnerability* atau celah *server* terlihat	Berhasil atau Tidak

Pada UAT pengujian ini dilakukan dengan melihat hasil dari implementasi rancangan infrastruktur backup data pada PT. Global Media Utama Teknologi.

Tabel 3 1 User Acceptance Test

NO	Pengujian	Ekspetasi	Catatan
1	Pengguna dapat masuk kedalam NAS	Sesuai atau Tidak	
2	Pengguna dapat membuat folder di dalam NAS	Sesuai atau Tidak	
3	Aplikasi *backup acronis cyber protect* berhasil di *install* pada *server*	Sesuai atau Tidak	
4	*Administrator* dapat masuk kedalam aplikasi backup *acronis cyber protect*	Sesuai atau Tidak	
5	*Administrator* dapat membuat *policy backup*	Sesuai atau Tidak	

6	*Administrator* dapat melihat *report backup*	Sesuai atau Tidak	
7	*Administrator* dapat melihat *report virus* yang terdeteksi	Sesuai atau Tidak	
8	*Administrator* dapat menjeda *backup* yang sedang berlangsung	Sesuai atau Tidak	
9	*Administrator* dapat melanjutkan *backup* yang terjeda	Sesuai atau Tidak	
10	*Administrator* dapat melihat *guest agent acronis* yang sedang berjalan	Sesuai atau Tidak	

3.2.4 Lingkungan Pengembangan

1. *Tools*

a. *Tools backup* yang digunakan adalah *acronis cyber protect versi 16.*

b. *server* yang di gunakan untuk aplikasi *backup acronis cyber protect* dengan spesifikasi : *Intel Xeon E5-2630v4*, *RAM 8GB,* dan storage sebesar 100GB.

c. Sistem Operasi menggunakan *Windows Server 2016* sebagai tempat dari *acronis cyber protect.*

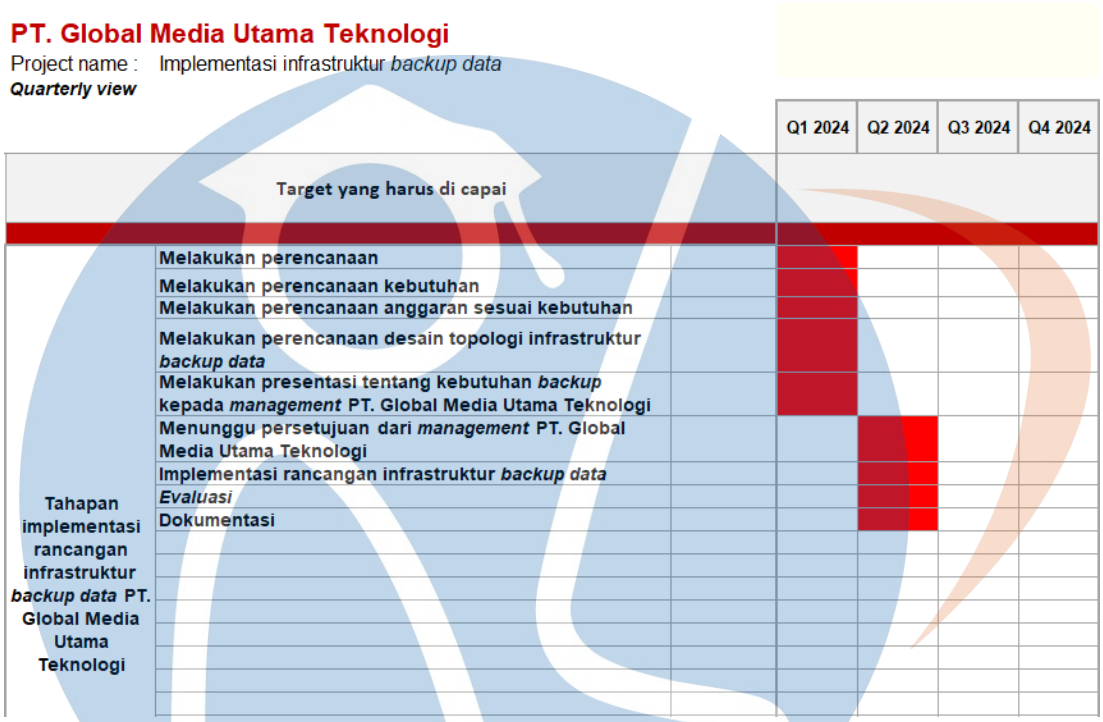
d. *NAS (Network Attached Storage)* menggunakan *TrueNAS, RAM, CPU 4 Core, 8GB, HDD 4TB*

e. *Browser* menggunakan *Microsoft Edge*

f. Protokol *SMB(Server Message Block)* sebagai koneksi antara *NAS* dengan *server acronis cyber protect*

3.2.5 Waktu Penelitian (*Gantt Chart*)

Pada tahapan ini penulis memberikan gambaran waktu penelitian yang dibutuhkan oleh penulis. Dengan rentang waktu penelitian kuartal 1 hingga kuartal 4 tahun 2024 . Berikut untuk waktu penelitian yang di butuhkan penulis :



Gambar 3 Waktu Penilitian

3.2.6 Metode Implementasi dan Evaluasi

Penerapan rancangan infrastruktur *backup* yang akan diimplementasikan di PT. Global Media Utama Teknologi, dilakukan secara bertahap. Implementasi dimulai dengan perencanaan kebutuhan, perencanaan topologi, perencanaan jadwal implementasi, dan evaluasi dari implementasi infrastruktur *backup*. Selama implementasi juga dilakukan evaluasi yang berkelanjutan untuk mendeteksi dan mengatasi masalah yang mungkin muncul. Setelah implementasi selesai, maka di lakukan evaluasi kembali dengan menilai keseluruhan kinerja dari implementasi yang sudah dilakukan, antara lainnya pengukuran pencapaian tujuan, kepuasan pengguna

BAB IV
IMPLEMENTASI DAN EVALUASI

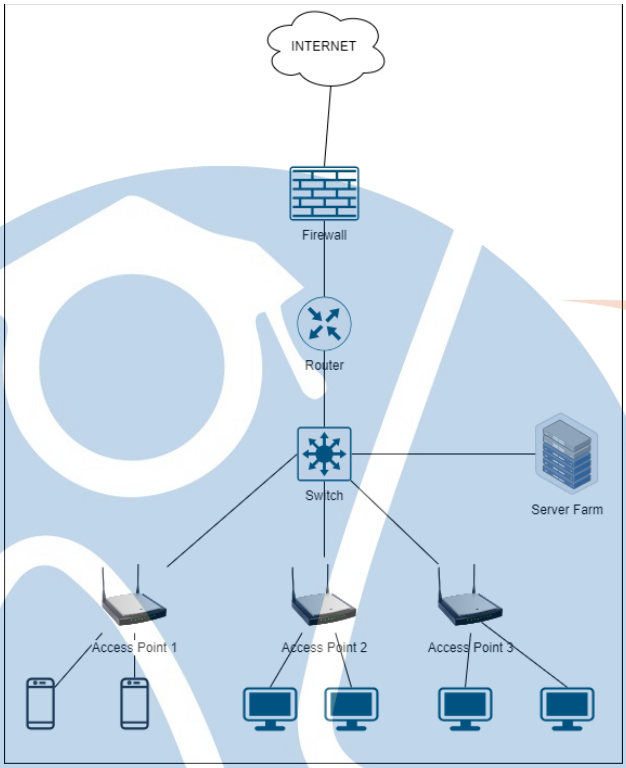
4.1. Analisis Sistem

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 Analisa ini bertujuan untuk melakukan identifikasi perangkat yang saat ini berjalan, supaya saat implementasi *backup data* tidak terjadi gangguan atau terhentinya oprasional perusahaan PT. Global Media Utama Teknologi, lalu mengetahui *data* apa saja yang akan dilakukan *backup*, selanjutnya menambah keamanan pada infrastruktur *backup*.

4.1.1 Topologi saat ini

Dari hasil analisa sebelumnya, maka didapatkan topologi saat ini adalah



Gambar 4 1 Topologi saat ini

4.1.2 Daftar perangkat

Daftar perangkat yang terdapat pada perusahaan PT. Global Media Utama Teknologi :

Table 4 1 Daftar perangkat

NO	Nama Perangkat	IP Address	Fungsi
1	GUT-APP-CRM-OLD	192.168.8.2	Aplikasi CRM lama
2	GUT-Email	192.168.8.6	Server Email
3	GUT-SVR-AD	192.168.8.7	Server Active Directory
4	GUT-SVR-Antivirus-Kaspersky	192.168.8.8	Server Antivirus Kaspersky
5	GUT-SVR-Email-Gateway	192.168.8.10	Email Gateway Kaspersky Security
6	GUT-SVR-Backup	192.168.8.14	Server Acronis cyber protect management server

7	GUT-NAS-TrueNAS	192.168.8.15	GUT TrueNAS
8	GUT-Helpdesk	192.168.8.18	Server Helpdesk
9	GUT-SVR-Accurate	192.168.8.21	Server accounting untuk aplikasi Accurate
10	GUT-Ecommerce	192.168.8.30	Server Website Ecommerce GUT
11	GUT-APP-CRM	192.168.8.50	Aplikasi CRM baru
12	GUT-Firewall-Fortigate	192.168.8.254	Firewall Fortigate

4.1.3 Kebutuhan *Backup Data*

Dari analisa sebelumnya perusahaan ingin adanya *backup* untuk beberapa *data* penting antara lain :

Table 4 2 Kebutuhan *backup data*

NO	File/Folder/Host VM	Server IP	Server Hostname	Ukuran Total(GB)
1	D:/GUT2	192.168.8.21	SVR_Accurate	10 GB
2	D:/MCI	192.168.8.21	SVR_Accurate	8GB
3	D:/SDM	192.168.8.21	SVR_Accurate	2GB
4	Active-Directory	192.168.8.8	SVR_AD	512GB
5	Email-Server	192.168.8.6	SVR-Email	256GB
6	GUT-APP-CRM	192.168.8.51	GUT-APP-CRM	200GB
7	GUT-APP-CRM-OLD	192.168.8.2	GUT-APP-CRM-OLD	512GB
8	GUT-WEB-Ecommerce	192.168.16	GUT-WEB-Ecommerce	256GB

4.1.4 *Role Account*

Mempertimbangkan sisi keamanan perusahaan ingin adanya *role Account* atau kategori peran pada sistem *backup* :

Table 4 3 Role Account

NO	Perangkat	peran	pengguna
1	*TrueNAS*	*Administrator*	*IT*
2	*TrueNAS*	*Read Only*	*auditor*
3	*Acronis Cyber Protect Management Server*	*Administrator*	*IT*

4	*Acronis Cyber Protect Management Server*	*Read Only*	*Auditor*

4.1.5 Pembatasan perangkat

Perusahaan ingin adanya pembatasan perangkat yang boleh terhubung dengan infrastruktur *backup* untuk mencegah terjadi kehilangan *data* hasil *backup.* Maka diterapkan pembatasan dari beberapa *IP Address* dan segmen pada table berikut :

Perangkat yang boleh terhubung ke *NAS* adalah sebagai berikut :

Table 4 4 Pembatasan perangkat

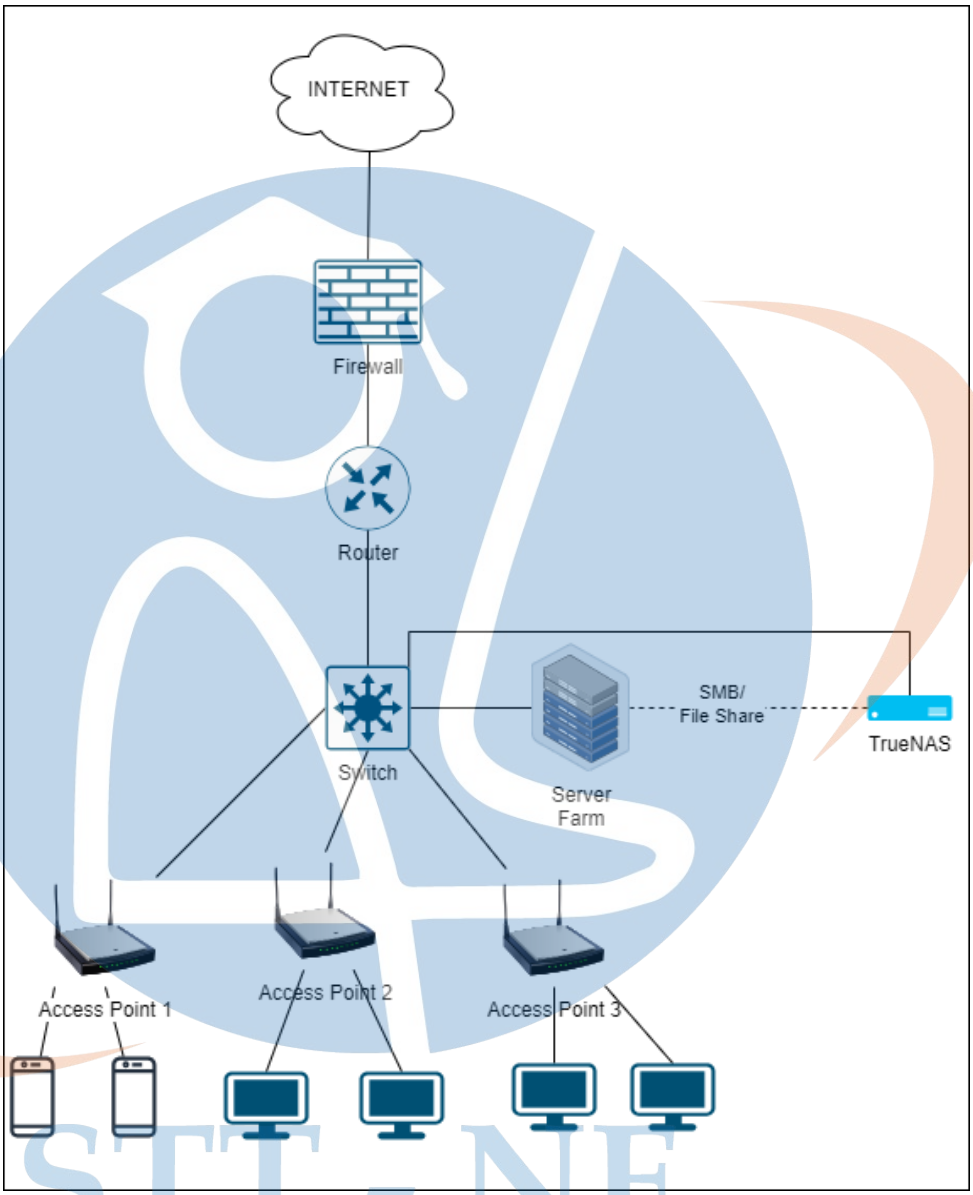
	Dari				Tujuan	
NO	Perangkat/Segmen	IP Address	Port yang diizinkan	Service yang dipergunakan	Tujuan	Perangkat
1	*GUT-Accurate*	*192.168.8.21*	*445, 138,139*	*SMB File/Folder share*	*192.168.8.15*	*GUT-NAS-TrueNAS*
2	*GUT-Active Directory*	*192.168.8.7*	*445, 138, 139*	*SMB File/Folder share*	*192.168.8.15*	*GUT-NAS-TrueNAS*
3	*SVR-Email*	*192.168.8.6*	*445, 138,139*	*SMB File/Folder share*	*192.168.8.15*	*GUT-NAS-TrueNAS*
4	*GUT-APP-CRM*	*192.168.8.50*	*445, 138,139*	*SMB File/Folder share*	*192.168.8.15*	*GUT-NAS-TrueNAS*
5	*GUT-APP-CRM-OLD*	*192.168.8.2*	*445, 138,139*	*SMB File/Folder share*	*192.168.8.15*	*GUT-NAS-TrueNAS*
6	*GUT-WEB-Ecommerce*	*192.168.30*	*445, 138,139*	*SMB File/Folder share*	*192.168.8.15*	*GUT-NAS-TrueNAS*
7	*Perangkat pengguna*	*192.168.2.0/24*	*445, 138, 139*	*SMB File/Folder share*	*192.168.8.15*	*GUT-NAS-TrueNAS*

4.2 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 dimana 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* .

4.2.1 Desain Sistem

1. Topologi Implementasi

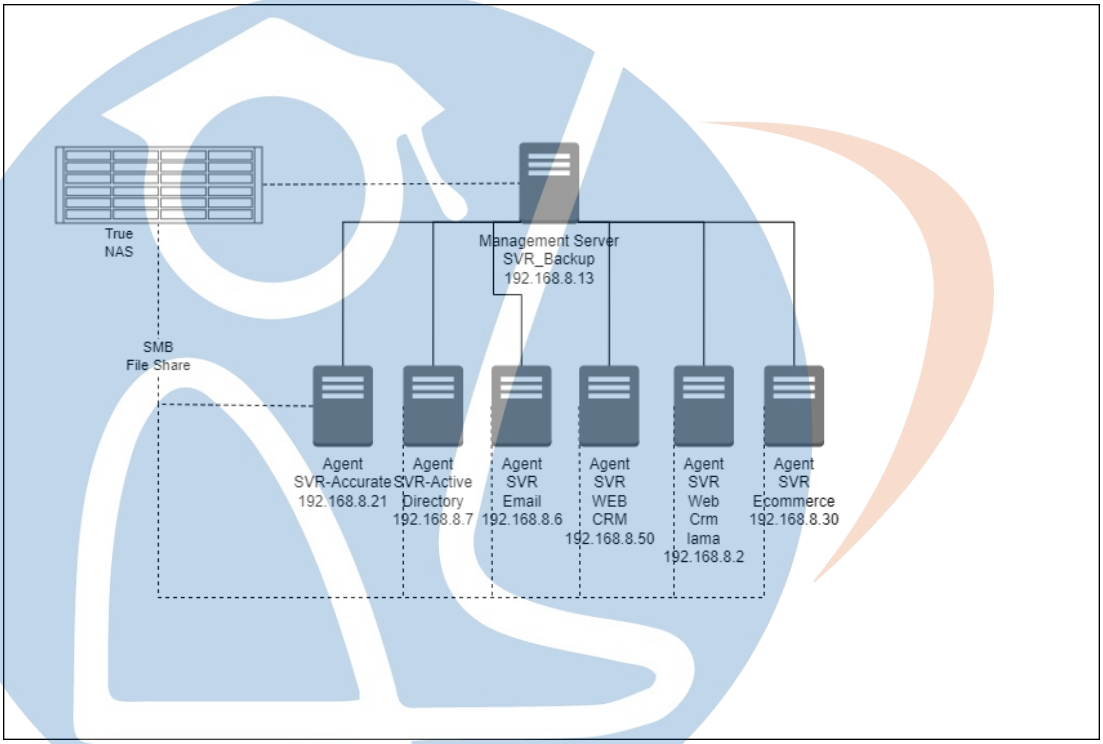


Gambar 4 2 Topologi Implementasi

Gambar diatas adalah menggambarkan topologi yang akan diimplementasikan, dengan melakukan pemisahaan *TrueNAS* diluar *server farm* dan dilakukan *filtering* terhadap koneksi yang terhubung ke *NAS.* Selanjutnya untuk server *Acronis Cyber Protect* ada didalam *server farm.* Dengan menerapkan pemisahan antara *Server farm* dengan *TrueNAS* bisa melindungi dari kehilangan *backup*.

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.*



Gambar 4 3 Acronis Management Server & Acronis Agent Server

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 table strategi *backup*.

Gambar 4 4 Strategi *backup*

NO	File/Folder/Host VM	Server IP	Server Hostname	Ukuran Total (GB)	Tipe Backup dan Jadwal Backup		
					Incremental backup	Diffrential backup	Full backup
1	D:/GUT2	192.168.8.21	SVR_Accurate	10 GB	Setiap hari dalam 1 Minggu di jam 19:00		1 Bulan sekali di tanggal 29 setiap bulan
2	D:/MCI	192.168.8.21	SVR_Accurate	8GB	Setiap hari dalam 1 Minggu di jam 21:00		1 Bulan sekali di tanggal 29 setiap bulan
3	D:/SDM	192.168.8.21	SVR_Accurate	2GB	Setiap hari dalam 1 Minggu di jam 22:30		1 Bulan sekali di tanggal 29 setiap bulan
4	Active-Directory	192.168.8.7	SVR_AD	512GB			1 Bulan sekali di tanggal 10 setiap bulan
5	Email-Server	192.168.8.6	SVR-Email	256GB	Seminggu 1x pada hari selasa di jam 20:00		1 Bulan sekali di tanggal 15 setiap bulan

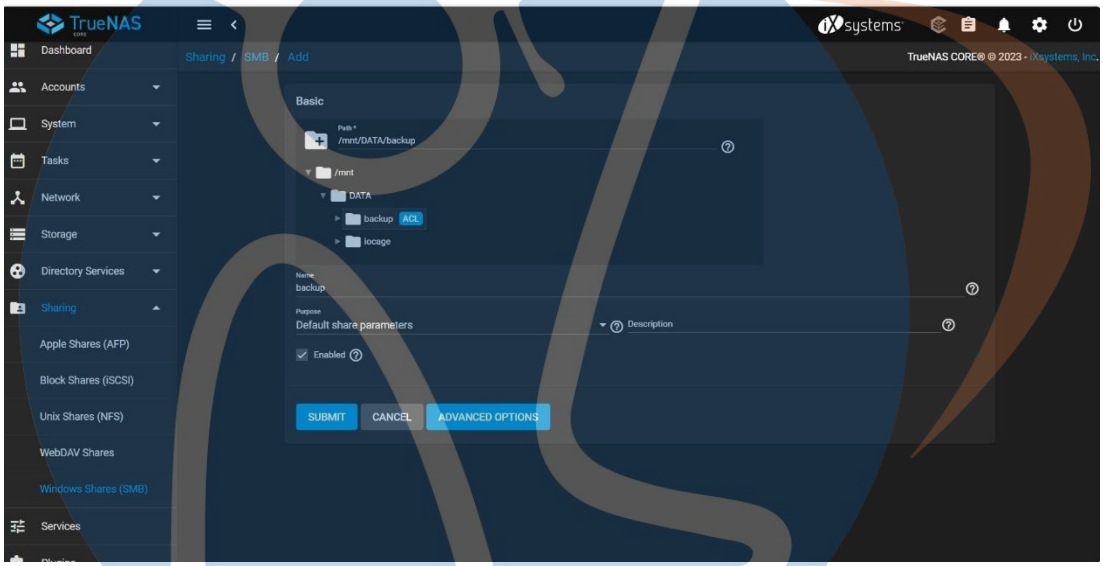
6	GUT-APP-CRM	192.168.8.51	GUT-APP-CRM	200GB	Seminggu 1x pada hari kamis di jam 20:00		1 Bulan sekali di tanggal 14 setiap bulan
7	GUT-APP-CRM-OLD	192.168.8.2	GUT-APP-CRM-OLD	512GB			1x setiap tahun pada bulan januari di tanggal 15
8	GUT-WEB-Ecommerce	192.168.16	GUT-WEB-Ecommerce	256GB	Seminggu 2x pada hari sabtu dan minggu di jam 22:00		1 Bulan sekali di tanggal 20 setiap bulan

4.3 Implementasi

4.3.1 Implementasi *TrueNAS*

Untuk menampung hasil *backup* maka diperlukan untuk membuat *folder* hasil *backup* didalam *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.

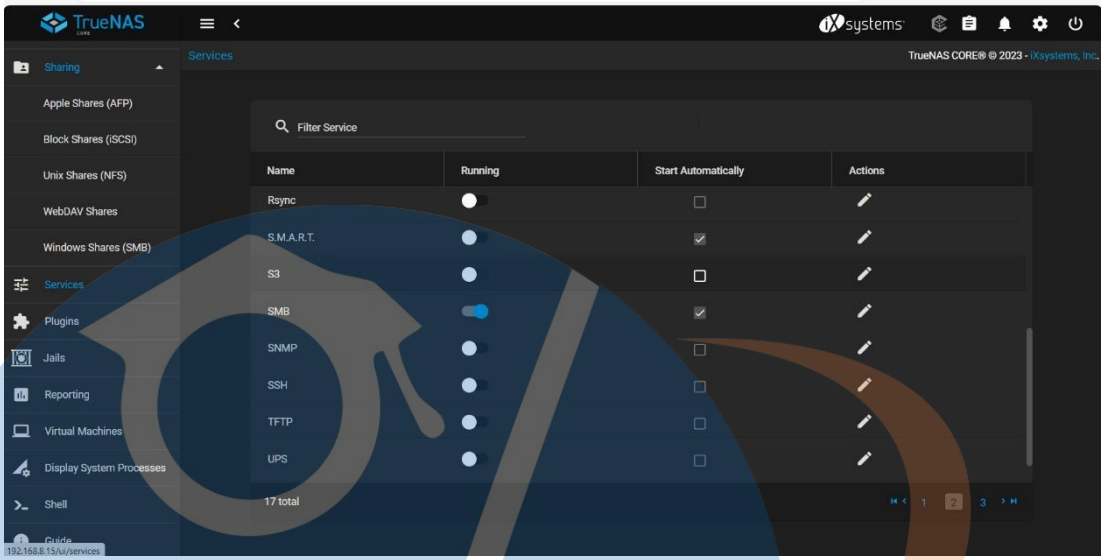
1. Membuat *folder share*



Gambar 4 5 Membuat *folder share*

Folder share 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 protocol *SMB (Server Message Block).*

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



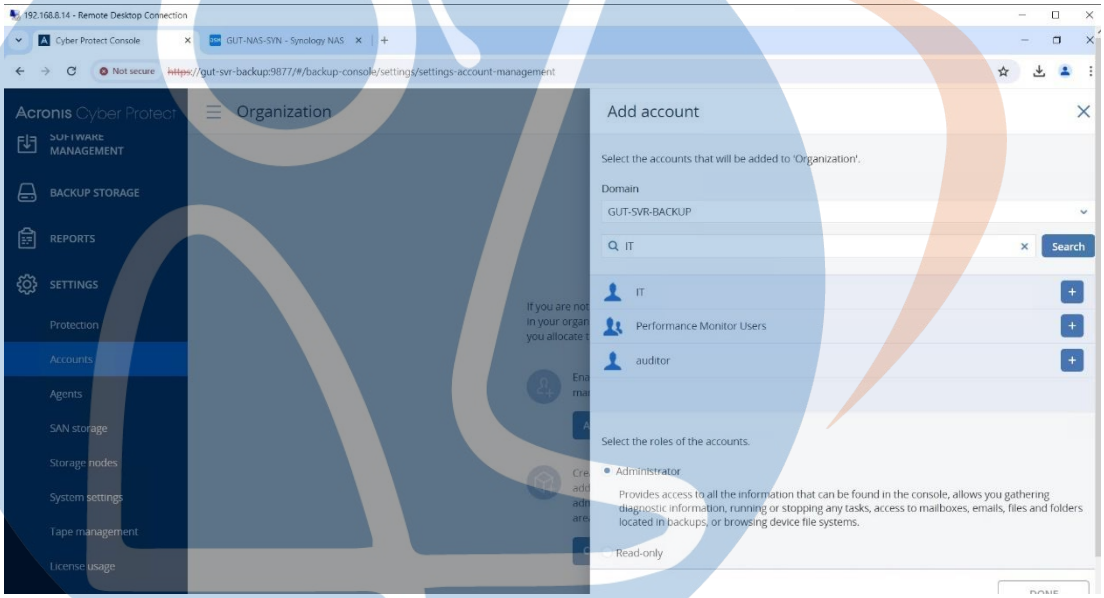
Gambar 4 6 Mengaktifkan *service SMB (Server Message Block)*

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)*.

4.3.2 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*.

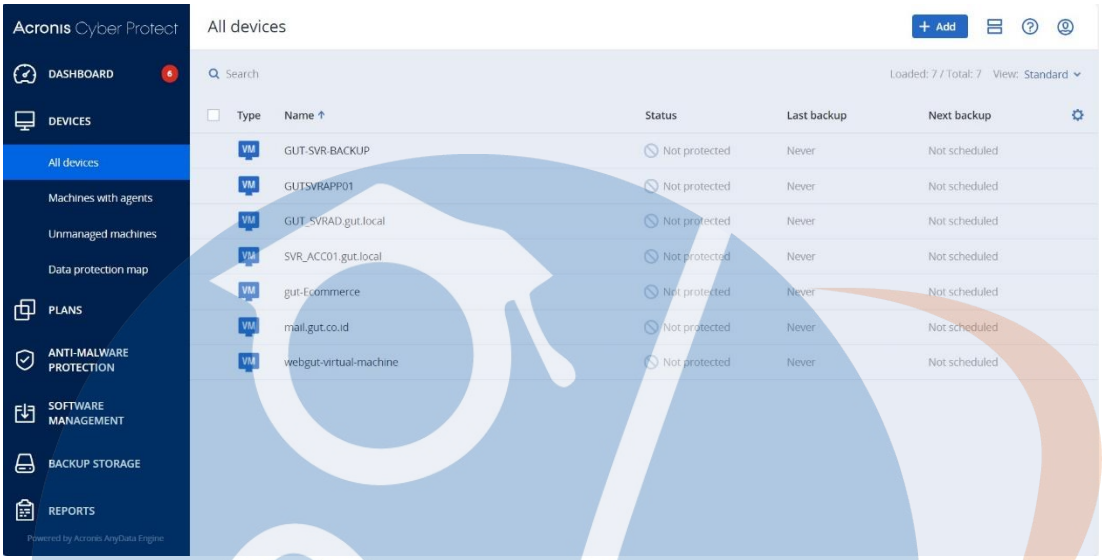
1. Menambahkan pengguna *Acronis Cyber Protect*



Gambar 4 7 menambahkan pengguna acronis cyber protect

Perusahaan menginkan adanya pembatasan akses ke *server Acronis Cyber Protect* sesuai dengan kriteria yang sudah ditentukan sebelumnya. Pada pembatasan ini pengguna *IT* memiliki akses *Administrator* yang memiliki akses penuh terhadap *Acronis Cyber Protect*. Selanjutnya untuk pengguna *auditor*, memiliki akses hanya baca saja, tidak bisa melakukan konfigurasi.

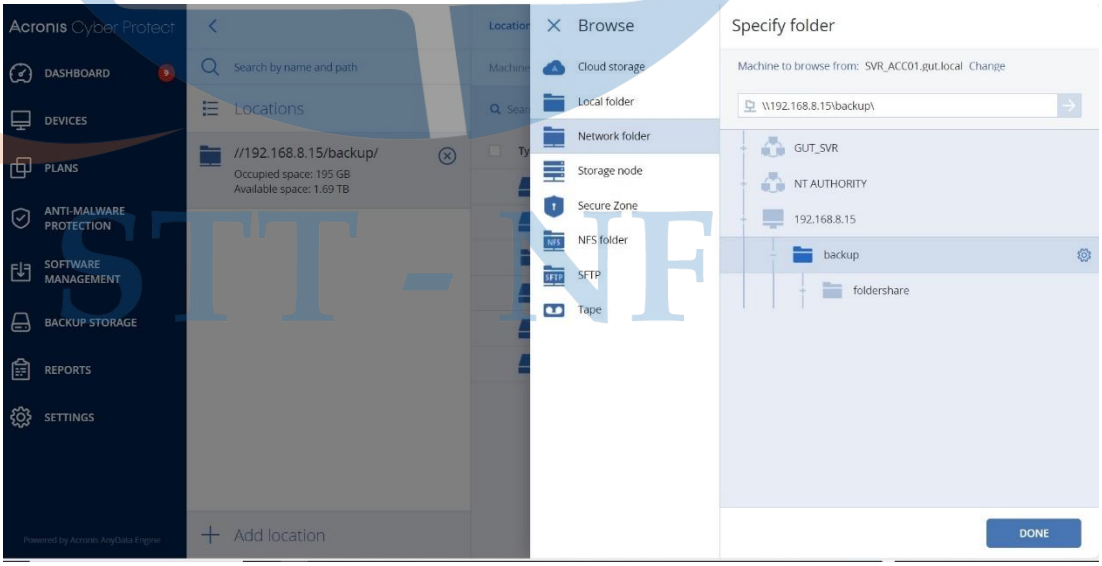
2. Menambahkan *server* yang akan melakukan *backup*



Gambar 4 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* disini sudah terdapat *server* yang sudah terpasang aplikasi *Agent* dari aplikasi *Acronis Cyber Protect*.

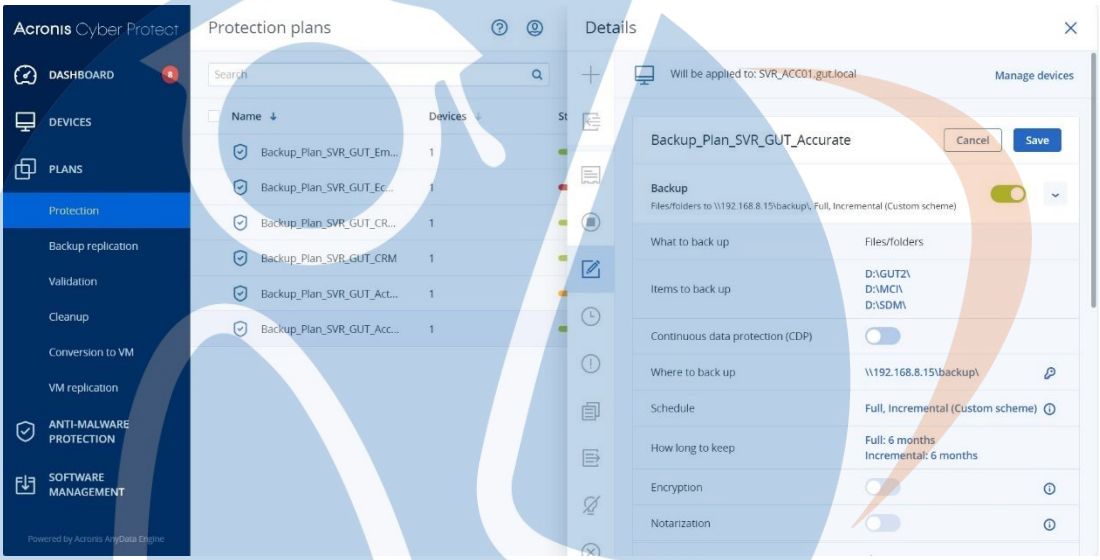
3. Menentukan lokasi tempat penyimpanan hasil *backup*



Gambar 4 9 Menentukan lokasi tempat penyimpanan hasil backup

Untuk menyimpan hasil *backup*, diperlukan adanya *koneksi* dari *Agent* yang terinstall 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.

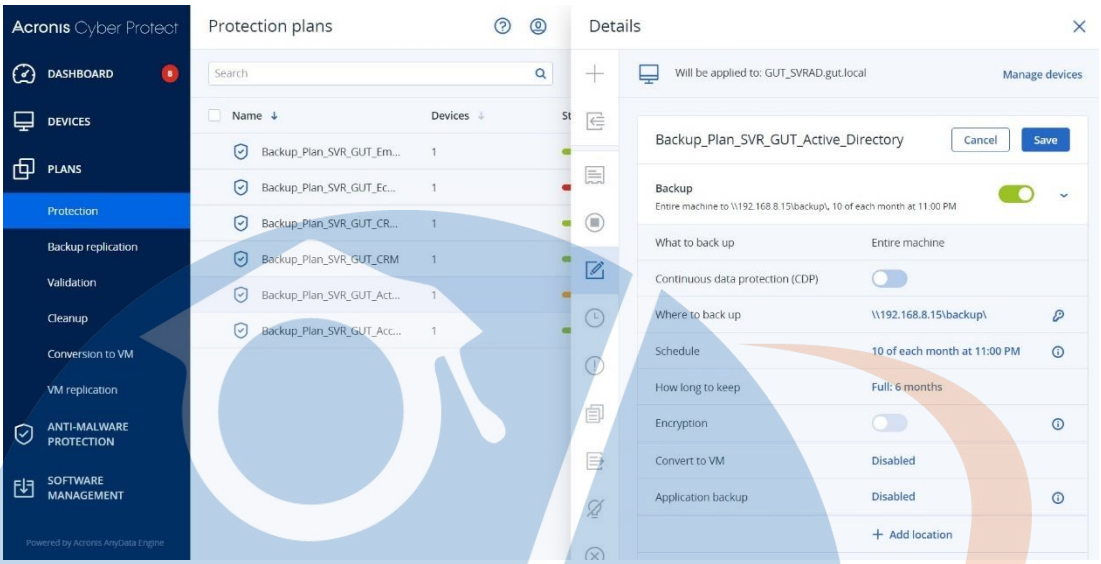
4. Membuat jadwal *backup serverAccurate*



Gambar 4 10 membuat jadwal backup server accurate

Untuk *backup* bisa dilakukan nya *backup* secara otomatis dan terjadwal di perlukan adanya sebuah *Plans* pada *agent acronis* yang terinstall. 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.

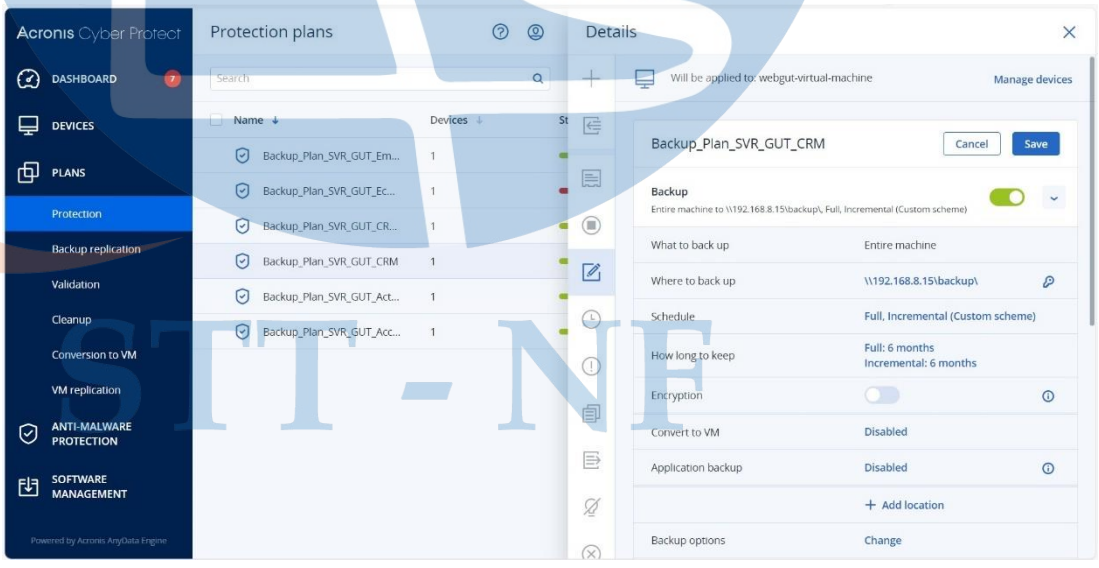
5. Membuat jadwal *backup server Active Directory*



Gambar 4 11 Membuat jadwal backup server active directory

Selanjutnya *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).

6. Membuat jadwal *backup server GUT CRM*

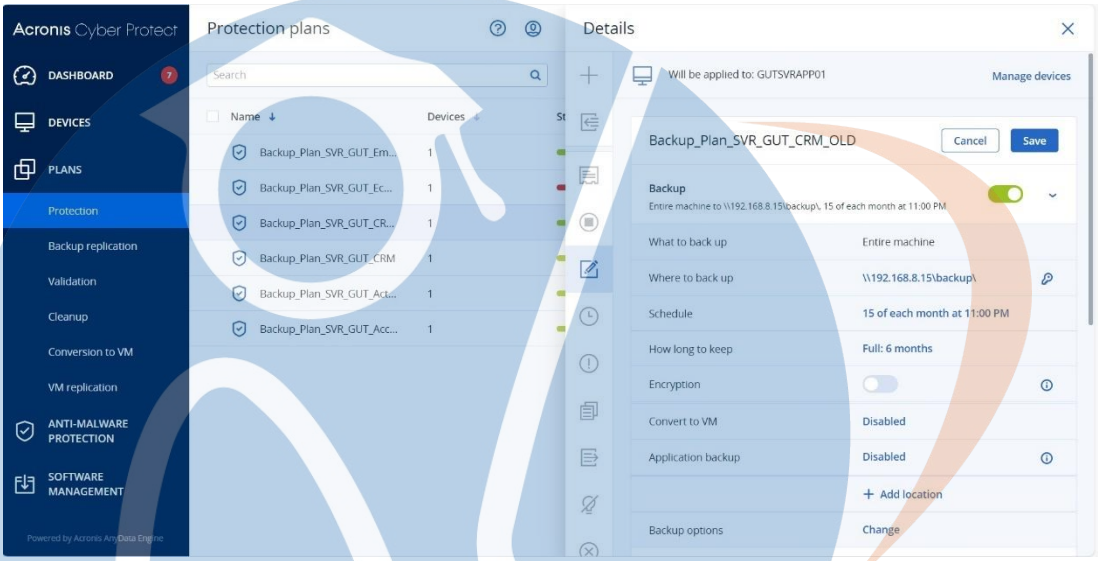


Gambar 4 12 Membuat jadwal backup server GUT CRM

Selanjutnya *server GUT CRM (Customer Relationship Management)* sangat penting karena didalam *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.

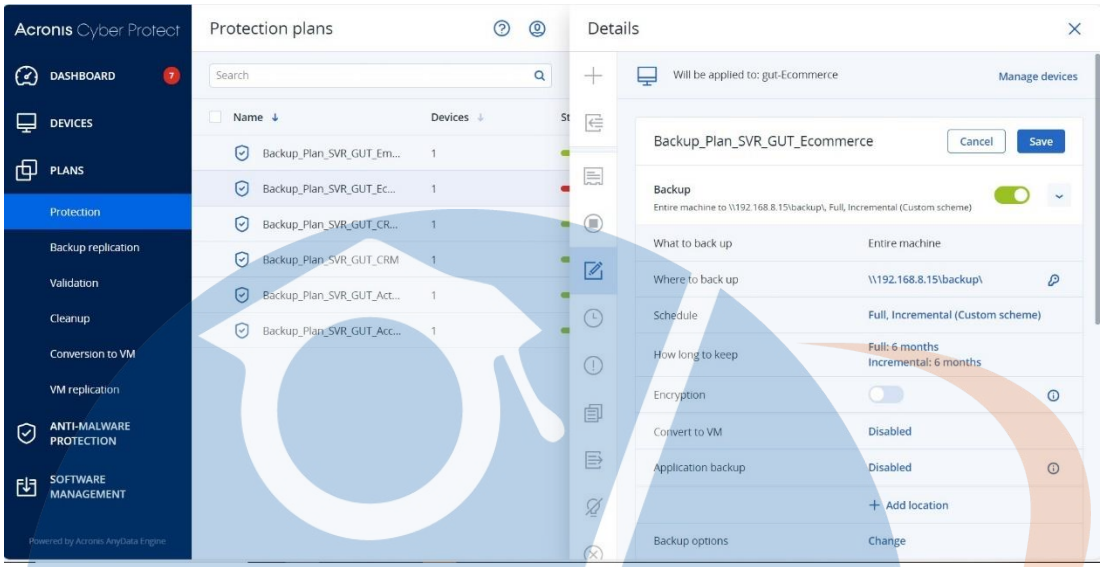
7. Membuat jadwal *backup server GUT CRM OLD*



Gambar 4 13 Membuat jadwal backup server GUT CRM OLD

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.

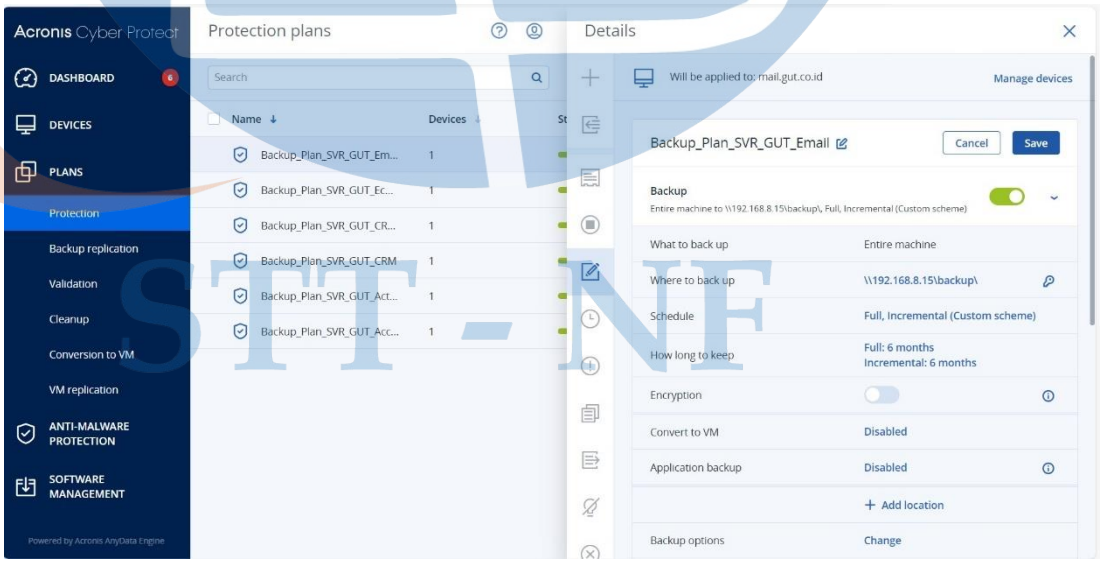
8. Membuat jadwal *backup server GUT Ecommerce*



Gambar 4 14 Membuat jadwal backup server GUT Ecommerce

Pembuatan *plans backup* juga dilakukan pada *server GUT Ecommerce* dengan metode *incrementall backup* 2 kali pada hari sabtu dan minggu disetiap minggu nya dijam 22:00, Selanjutnya metode *full backup* dilakukan 1kali sebulan pada setiap tanggal 20.

9. Membuat jadwal *backup server email*



Gambar 4 15 Membuat jadwal backup server Email

Email adalah surat elektonik 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 dijam 20:00, dan satu bulan sekali pada tanggal 14 setiap bulannya.

4.4 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*, dan *User Acceptance Testing* (UAT).

4.4.1 Hasil Black Box Testing

Table 4 5 Hasil black box testing

NO	Pengujian	Ekspetasi	Hasil
1	*NAS(Network Attached Storage) berfungsi dengan baik sesuai harapan*	*NAS* dapat berfungsi dengan baik	Berhasil
2	*Harddisk* di pasang kedalam 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* kedalam aplikasi *Acronis Cyber Protect*	*Folder sharing backup* berhasil di tambahkan	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

4.4.2 Hasil UAT

Table 4 6 Hasil UAT

NO	Pengujian	Ekspetasi	Catatan
1	Pengguna dapat masuk kedalam 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	Sesuai	-

	report virus yang terdeteksi		
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	-

4.4.3 Hasil *Backup*

Table 4 7 Hasil Backup

No	*Server/Virtual Machine*	tipe kompresi	byte data yang di proses	byte data yang berhasil di backup	rasio kompresi	Waktu yang di perluka 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* diatas, 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 :

Presentasase rasio = (*Byte* yang diproses / *Byte* data yang berhasil di *backup*) x 100%

4.4.4 Hasil Restore

Table 4 8 Hasil Restore

No	*Server/Virtual Machine*	tipe backup	jenis backup	byte data yang di proses	Waktu yang di perluka untuk restore	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*.

BAB V
KESIMPULAN DAN SARAN

5.1 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,* konfiguasi *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 keaman *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 transmisi nya, 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 ketidak sengajaan saat operasional perusahaan sedang berlangsung.

5.2 Saran

Berdasarkan penelitian, implementasi, dan uji coba. Penulis menyarankan beberapa pengembangan dalam rancangan infrastruktur *backup,* dengan fokus pada :

1. Perlu dilakukan pengembangan *backup* ke teknologi *Disaster Recovery* untuk mencegah terjadinya *Down* pada sistem/aplikasi perusahaan yang akan mengakibatkan kerugian perusahaan setiap menitnya.
2. Perlu dilakukan enkripsi pada data yang sudah dilakukan *backup* untuk mencegah terjadinya kebocoran data akibat serangan siber ataupun kesengajaan didalam lingkup perusahaan.
3. Perlu adanya *backup off-site* untuk mengamankan data yang sudah berhasil dilakukan *backup* ke tempat terpisah, untuk mecegah terjadinya kehilangan file *backup* secara menyeluruh jika terjadi serangan siber.
4. Perlu dilakukan monitoring terhadap konsistensi hasil *backup* yang sudah berhasil, untuk mencegah terjadinya kegagalan saat melakukan *recovery/restore file.*

   Saran pengembangan tersebut dapat menjadi panduan untuk melakukan penelitian selanjutnya guna memastikan terus berkembanganya keamanan data yang terkini dan relevan sesuai dengan tren keamanan siber

DAFTAR REFERENSI

[1] D. A. Arifah, "KASUS CYBERCRIME DI INDONESIA," *Jurnal Bisnis dan Ekonomi (JBE)*, vol. 18, 2011.

[2] M. I. P. N. Zahrani Fatni Hapsah, "ANALISIS TINGKAT KEAMANAN DATA PERUSAHAAN YANG RENTAN TERHADAP SERANGAN CYBER DALAM SISTEM INFORMASI MANAJEMEN," *Jurnal Manajemen Dan Akuntansi*, vol. 1, pp. 338-343, 2023.

[3] S. Muhamad Danuri, "TREND CYBER CRIME DAN TEKNOLOGI INFORMASI DI INDONESIA," *INFOKAM*, 2017.

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

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

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

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

[8] 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.

[9] Acronis, "Acronis," [Online]. Available: https://www.acronis.com/id-id/company/. [Diakses 12 3 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] G. B. H. B. S. G. A. S. M. T. A. D. P. M. Widya Lelisa Army, Teknologi Jaringan Komputer, 2022.

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

[14] A. W. Ma’arij Haritsah, “Analisis Karakteristik Antivirus Berdasarkan Aktivitas Malware Menggunakan Analisis Dinamis,” *Journal of Information System Research*, vol. 4, 2023.

[15] W. w. t. S. Aidil., “STUDI SISTEM KEAMANAN KOMPUTER,” *Jurnal Artificial, ICT Research Center UNAS,* vol. 2, 2008.

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

[17] W. I. Fahrullah, “ANALISIS BLACKBOX TESTING DAN USER ACCEPTANCE TESTING TERHADAP SISTEM INFORMASI SOLUSIMEDSOSKU,” *Jurnal Teknosains Kodepena,* vol. 04, 2023.

[18] 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].

[19] Truenas, “Truenas,” [Online]. Available: https://www.truenas.com/faq/. [Diakses 3 maret 2024].

[20] 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].

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

STT - NF

LAMPIRAN

Berisi antara lain: instrumen penelitian, surat keterangan telah melakukan penelitian dari obyek penelitian, dan lain-lain yang keterangan yang relevan.