JURNAL ILMU KOMPUTER
Volume 4 Nomor 1, Januari, 2026
ISSN: 3031-125X (ONLINE)
Penerbit: Program Studi Teknik Informatika S-2 Universitas Pamulang

# Analisa Backup Dan Replikasi Virtual Server Dengan Menggunakan Penjadwalan Koneksi Data Pada *Disaster Recovery Center* (DRC)

Bayu Putra Pratama [1], Taswanda Taryo [2], Achmad Hindasyah [3]

[1,2,3)] Teknik Informatika S-2, Program Pascasarjana, Universitas Pamulang, Kota Tangerang Selatan, Banten

[3)] Badan Riset dan Inovasi Nasional, Tangerang Selatan, Banten

Email: [1]bayuputra180708@gmail.com, [2]dosen02234@unpam.ac.id, [3]dosen00121@unpam.ac.id

***ABSTRACT***

*Server backup and replication are critical components in ensuring operational continuity and disaster recovery within modern information systems. One of the main challenges faced is the unscheduled transfer of data between the Data Center (DC) and the Disaster Recovery Center (DRC), which can lead to the spread of viruses, malware, and ransomware into the DRC environment, thereby disrupting the recovery process. This study aims to analyze the effectiveness of data connection scheduling in the backup and replication of virtual servers at PT XYZ Finance. The research adopts a quantitative approach by measuring system performance before and after the implementation of scheduled replication. Quantitative parameters include replication time, volume of successfully transferred data, backup success rate, and recorded security incidents. Data were collected through direct system testing and analyzed using descriptive and comparative statistical methods. The results show that implementing a structured data connection schedule in the replication system significantly supports faster operational recovery and reduces the number of security incidents impacting the DRC. Based on these findings, scheduled data connections in server replication have proven to be quantitatively effective in improving system efficiency and security. Therefore, this approach is recommended as part of a data-driven disaster recovery strategy in enterprise IT environments.*

*Keywords: Backup Virtual Server, Disaster Recovery Center (DRC), Replication Server, Schedulling data connecti, System Availability.*

**ABSTRAK**

*Backup* dan replikasi server merupakan bagian penting dalam menjaga kesinambungan operasional dan pemulihan bencana di lingkungan sistem informasi modern. Salah satu tantangan utama yang dihadapi adalah tidak terjadwalnya transfer data antara *Data Center* (DC) dan *Disaster Recovery Center* (DRC), yang berpotensi menyebabkan penyebaran virus, *malware*, dan ransomware ke lingkungan DRC, sehingga mengganggu proses pemulihan. Penelitian ini bertujuan untuk menganalisis efektivitas penjadwalan koneksi data dalam sistem backup dan replikasi server virtual di PT XYZ *Finance*. Penelitian menggunakan pendekatan kuantitatif, dengan mengukur performa sistem sebelum dan sesudah penerapan penjadwalan replikasi berdasarkan parameter kuantitatif seperti waktu replikasi, volume data yang berhasil ditransfer, tingkat keberhasilan *backup*, serta tingkat insiden keamanan yang tercatat. Data dikumpulkan melalui pengujian sistem secara langsung dan dianalisis menggunakan metode statistik deskriptif dan komparatif. Hasil penelitian menunjukkan bahwa penerapan sistem replikasi dengan penjadwalan koneksi data yang terstruktur mampu mendukung pemulihan operasional perusahaan dengan cepat, serta menurunkan tingkat insiden keamanan yang berdampak ke DRC secara signifikan. Berdasarkan hasil tersebut, penjadwalan koneksi data dalam replikasi server terbukti efektif secara kuantitatif dalam meningkatkan efisiensi dan keamanan sistem. Oleh karena itu, pendekatan ini direkomendasikan sebagai bagian dari strategi pemulihan bencana berbasis data yang terukur di lingkungan teknologi informasi Perusahaan.

Kata kunci: *Backup Virtual Server*, *Disaster Recovery Center* (DRC), Replikasi Server, Penjadwalan Koneksi Data, Keandalan Sistem.

## 1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat menyebabkan perusahaan semakin bergantung pada sistem TI untuk mendukung operasional sehari-hari. PT XYZ Finance sebagai perusahaan pembiayaan membutuhkan *Disaster Recovery Center* (DRC) yang didukung sistem *backup* dan replikasi data serta pembatasan koneksi jaringan antara *Data Center* (DC) dan DRC guna menjamin keberlangsungan operasional dan meminimalkan risiko serangan siber. Sistem pencadangan data menjadi komponen krusial dalam DRP karena memastikan ketersediaan data terbaru yang aman dan dapat digunakan saat terjadi bencana. Mengingat data merupakan aset penting perusahaan yang rentan terhadap kerusakan, kehilangan, maupun gangguan akibat faktor teknis dan nonteknis, diperlukan manajemen backup data yang tepat dan andal sebagai bagian dari penerapan *Disaster Recovery Plan*. [1]-[3]

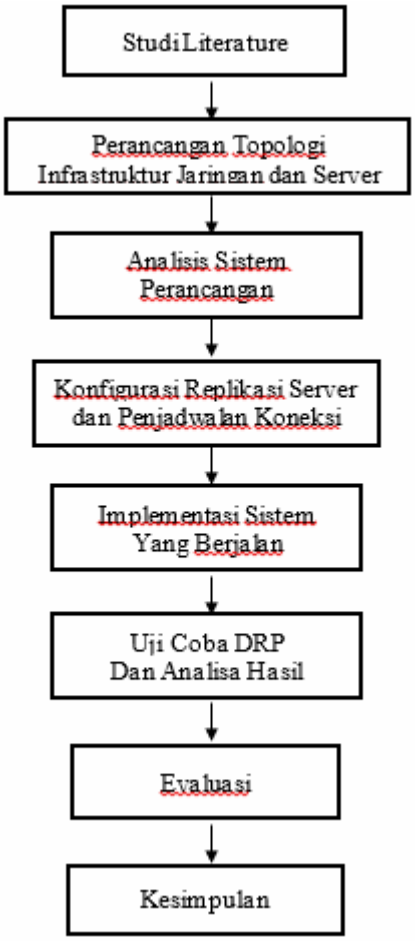
*Disaster Recovery Center* merupakan bagian integral dari *Disaster Recovery Plan* (DRP) dan *Business Continuity Plan* yang berfungsi menyediakan prosedur untuk merespons gangguan akibat bencana, menjalankan operasi cadangan, serta mengelola proses pemulihan sistem informasi secara cepat dan terukur. DRP bertujuan menjaga kelangsungan proses vital serta meminimalkan kerugian organisasi, sehingga harus dirancang secara sistematis dan tepat. Melalui penerapan prosedur pemulihan yang efektif, DRP memungkinkan sistem kritis dijalankan di lokasi alternatif dan dikembalikan ke kondisi normal dalam batas waktu yang dapat diterima. [4], [5]

Replikasi *server* merupakan proses penyediaan salinan data atau sistem di lokasi berbeda untuk meningkatkan ketersediaan, kinerja, dan toleransi terhadap kegagalan. Proses ini memerlukan manajemen yang baik guna menjaga konsistensi data, mencegah konflik, dan memastikan keamanan replikas. [6]-[8]

## 2. METODE

### 2.1. Tahapan Penelitian

Metode penelitian yang digunakan yaitu metode eksperimen dimana dilakukan percobaan menggunakan Software Veeam dan Firewall Fortigate. Adapun tahapan penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:

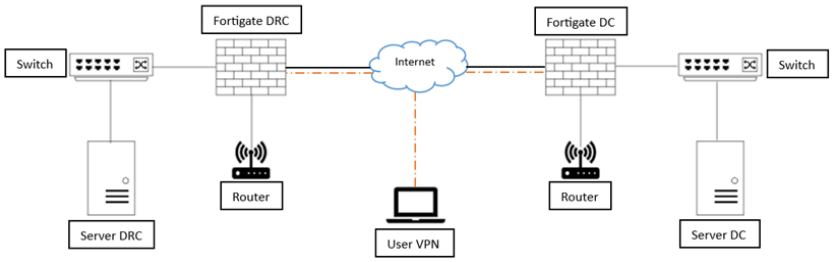



Gambar 1. Tahapan Penelitian

## 2.2. Perancangan Topologi Infrastruktur Jaringan dan Server

Topologi yang digunakan dalam membangun sistem replikasi ini yaitu menggunakan topologi *Star* dimana dalam topologi *star* tersebut menggunakan 2 buah *Firewall* Fortigate sebagai penghubung antar lokasi *server*. Adapun kelebihan topologi *star* adalah lebih hemat biaya untuk kabel jaringan. Kemudian, kegagalan pengiriman data pada satu rute tidak akan mempengaruhi rute yang lain. *Layout* jaringan atau topologi jaringan dimaksudkan untuk merancang topologi yang kiranya sesuai dengan sistem yang dikembangkan, sehingga gambaran topologi berikut dapat memberikan gambaran secara jelas tentang sistem yang hendak dibangun.[9], [10]

### 2.2.1. Topologi Jaringan Sebelum Dilakukan Implementasi Replikasi *Server*

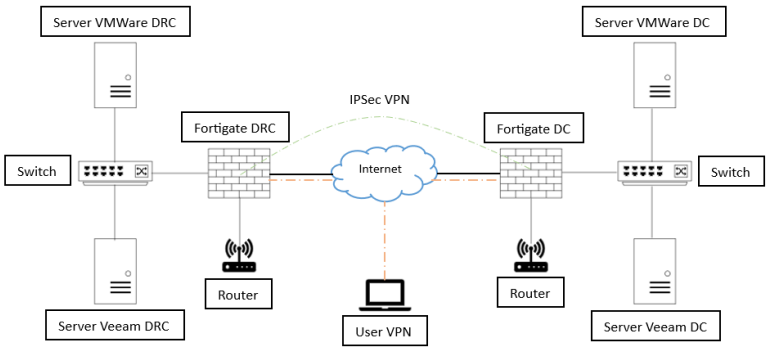



Gambar 2. Kondisi Jaringan Sebelum Dilakukan Implementasi Replikasi Server

Adapun penjelasan dari topologi jaringan dan infrastruktur *server* diatas adalah sebagai berikut :

1. Masing-masing *router* digunakan untuk memberikan akses internet dari pihak *provider* ke seluruh jaringan DC dan DRC yang didistribusikan melalui perangkat *firewall*.
2. *Switch* adalah suatu alat penghubung konektivitas antara perangkat *server* dan *firewall*.
3. Masing-masing site hanya memiliki satu *server* untuk seluruh layanan yang dijalankan.
4. Koneksi antara DC dan DRC terhubung secara terbuka melalui koneksi internet.
5. *Server* DC dan DRC saling terhubung terus menerus secara langsung untuk melakukan pemindahan data *backup*.
6. *User* yang menggunakan koneksi eksternal dapat terhubung menggunakan VPN ke DC dan DRC.

### 2.2.2. Topologi Jaringan Setelah Dilakukan Implementasi Replikasi *Server*




Gambar 3. Kondisi Jaringan Setelah Dilakukan Implementasi Replikasi *Server*

Adapun penjelasan dari topologi jaringan diatas adalah sebagai berikut:

1. Masing-masing *router* digunakan untuk memberikan akses internet dari pihak *provider* ke seluruh jaringan DC dan DRC yang didistribusikan melalui perangkat firewall.
2. Switch adalah suatu alat penghubung konektivitas antara perangkat *server*, *Server* Veeam dan *firewall*.
3. *Server* Veeam adalah perangkat komputer yang digunakan untuk menjalankan layanan sistem Veeam Backup & Replication.
4. *Server* adalah perangkat komputer yang menjalankan layanan komputasi kebutuhan perusahaan.
5. Infrastruktur jaringan DC & DRC terhubung menggunakan IPSec VPN.
6. *User* yang menggunakan koneksi eksternal dapat terhubung menggunakan VPN ke DC dan DRC.

## 2.3. Analisa Kebutuhan

### 2.3.1. Pengalokasian IP *Address*

Berikut merupkan pengalokasian IP *Address* yang ditunjukkan pada Tabel:

Tabel 1. *Pengalokasian IP Address*

| **Perangkat DC** | |
|---|---|
| **Perangkat** | **IP Address** |
| Firewall Fortigate | 103.xxx.xxx.30 |
| Switch | 192.xxx.x.6 |
| Server | 192.xxx.xx.21 |
| Server Veeam | 192.xxx.xx.24 |
| **Perangkat DRC** | |
| Firewal Fortigate | 103.167.178.50 |
| Switch | 192.168.14.2 |
| Server | 192.168.14.21 |
| Server Veeam | 192.168.14.22 |

### 2.3.2. Kebutuhan *Hardware*

Kebutuhan *hardware* ini digunakan dalam membangun topologi infrastruktur jaringan dan *server* sesuai dengan yang dirancang oleh penulis. Berikut merupakan tabel kebutuhan *hardware*:

Tabel 2. Kebutuhan *Hardware*

| **Lokasi DC** | | |
|---|---|---|
| **Jenis Perangkat** | **Spesifikasi** | **Jumlah** |
| Firewall Fortigate | - Fortinet Fortigate Firewall 201F | 1 |

| | | | |
|---|---|---|---|
| Server Rackmount | - | HPE DL160 gen10 | 1 |
| Server Rackmount | - | HPE DL160 gen10 | 1 |
| Switch | - | HP Procurve 2510G-24 J9279A 24Port | 1 |
| **Lokasi DRC** | | | |
| Firewall Fortigate | - | Fortinet Fortigate Firewall 201E | 1 |
| Server Rackmount | - | HPE DL180 Gen9 | 1 |
| Server Rackmount | - | HPE DL180 Gen9 | 1 |
| Switch | - | HP Procurve 2510G-24 J9279A 24Port | 1 |

2.3.3. Kebutuhan *Software*

*Software* adalah merupakan suatu program komputer yang berfungsi untuk melakukan tugasnya masing masing. Dalam penelitian ini berikut merupakan *software* yang digunakan adalah:

Tabel 3. Kebutuhan *Software*

| Nama | Spesifikasi | Keterangan |
|---|---|---|
| VMWare | Versi 8.0.1 | Sistem Virtualisasi Server |
| Veeam Backup & Replication | Build 12.1.2.172 | Sistem backup dan replikasi |
| FortiOS | Versi v7.2.8 build1639 (Mature) | Firewall Operating System |

## 3. HASIL DAN PEMBAHASAN

Sistem yang dikembangkan ini memberikan gambaran tentang penerapan sistem serta mengevaluasi efektivitas solusi dalam meningkatkan keandalan, keamanan, dan kontinuitas layanan teknologi informasi di perusahaan. Pembahasan dilakukan melalui pendekatan kuantitatif dan kualitatif berdasarkan hasil uji coba, observasi lapangan, serta pengukuran kinerja sistem.

### 3.1. Kondisi Sistem Sebelum Implementasi

Pada tahap awal penelitian, kondisi infrastruktur dan sistem *backup* PT. XYZ Finance masih berjalan secara *manual* dan belum terintegrasi dengan sistem *Disaster Recovery Center* (DRC) yang optimal. Hal ini menimbulkan beberapa kelemahan yang berdampak signifikan terhadap keamanan, keandalan, serta keberlanjutan operasional sistem informasi Perusahaan.

a. Proses Backup *Manual*
b. Tidak Adanya Penjadwalan Koneksi
c. Risiko Operasional

Kondisi ini menimbulkan kerentanan serius, terutama bagi PT. XYZ Finance yang sangat bergantung pada sistem informasi untuk operasional dan layanan kepada pelanggan. Oleh karena itu, dibutuhkan solusi menyeluruh yang mengintegrasikan replikasi *server*, dan penjadwalan koneksi data agar DRC dapat berfungsi secara optimal sebagai bagian dari *Disaster Recovery Plan* (DRP) Perusahaan.

## 3.2. Implementasi Sistem Replikasi dan Penjadwalan Koneksi Data

### 3.2.1. Desain dan Arsitektur Sistem Baru

Tahap perancangan sistem meliputi penyusunan topologi jaringan dan konfigurasi server antara Data Center (DC) dan Disaster Recovery Center (DRC) dengan memanfaatkan server fisik, Veeam Backup & Replication untuk backup dan replikasi virtual machine, serta firewall Fortigate guna pengaturan dan penjadwalan koneksi antar lokasi.

### 3.2.2. Penjadwalan Koneksi Data

Penjadwalan koneksi data antara *Data Center* (DC) dan *Disaster Recovery Center* (DRC) dilakukan dengan mengatur waktu aktif replikasi pada interval tertentu guna meningkatkan keamanan, mengendalikan lalu lintas jaringan, dan meminimalkan risiko penyebaran *malware* tanpa mengganggu kinerja operasional utama.

### 3.2.3. *Warm backup* dan Replikasi Virtual *Server*

Metode *backup* yang diterapkan menggunakan pendekatan *warm backup* dengan replikasi *real-time* atau *near real-time*, di mana data dan sistem pada *server* utama disinkronkan secara berkala ke DRC menggunakan replikasi berbasis *image-level* dan *snapshot* melalui Veeam dengan penjadwalan otomatis untuk menjaga performa *server* utama.

### 3.2.4. Integrasi dan Uji Implementasi

Proses implementasi dilakukan secara bertahap dengan tahapan sebagai berikut:

1. Instalasi Veeam Backup & Replication dan konfigurasi *job* replikasi.

2. Konfigurasi VPN dan jadwal koneksi Fortigate antar *site* (DC dan DRC).
3. Pengujian awal terhadap proses replikasi antar *server*.
4. Uji coba DRC untuk memastikan bahwa sistem DRC dapat mengambil alih peran sistem utama ketika terjadi gangguan.

### 3.3. Hasil Uji Coba Sistem DRC

#### 3.3.1. Pengujian Replikasi *Server*

Pengujian ini bertujuan untuk memastikan bahwa proses replikasi *data* dari *server* utama (DC) ke *server* cadangan (DRC) berjalan secara otomatis, konsisten, dan efisien. Parameter yang diamati meliputi:

1. Konsistensi *data*: *Data* yang direplikasi diverifikasi untuk memastikan tidak ada perubahan atau kehilangan *data* selama proses *transfer*.
2. Interval replikasi: Replikasi dilakukan setiap hari sabtu dimulai dari jam 09.45.
3. Durasi proses replikasi: Rata-rata waktu replikasi untuk satu *snapshot* VM selama 1 – 2 jam, tergantung pada ukuran *data* yang direplikasi.
4. Keberhasilan replikasi: Tingkat keberhasilan mencapai 100% untuk semua VM yang terdaftar pada *job* Veeam Backup & Replication.

#### 3.3.2. Pengujian Penjadwalan Koneksi

Pengujian penjadwalan koneksi dilakukan untuk memastikan bahwa koneksi VPN antara *Data Center* (DC) dan *Disaster Recovery Center* (DRC) hanya aktif sesuai jadwal yang ditetapkan, yakni setiap hari Sabtu pukul 09.30–16.00. Hasil pengujian menunjukkan koneksi dapat aktif dan terputus secara otomatis, meningkatkan efisiensi penggunaan *bandwidth* serta memperkuat keamanan jaringan dengan membatasi lalu lintas di luar waktu replikasi.

#### 3.3.3. Hasil Penjadwalan Koneksi Data dan Replikasi Server dari DC ke DRC

Penjadwalan koneksi data dibuat setiap hari sabtu dimulai sejak tanggal 28 Juni 2025 sampai dengan 19 Juli 2025.

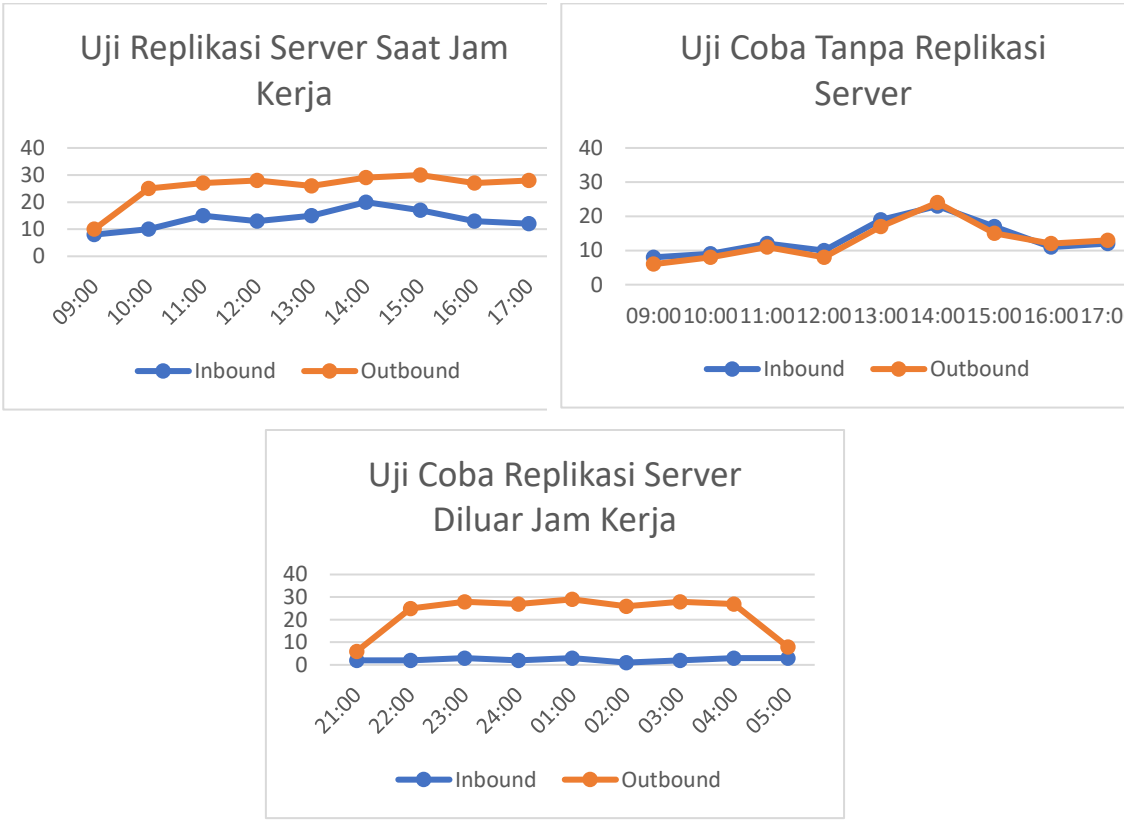
Tabel 4. Penjadwalan Koneksi Data pada *Firewall*

| **Tanggal** | **Jadwal Koneksi Data** |
|---|---|
| 28-Juni-2025 | 09.30 – 16.00 |
| 5-Juli-2025 | 09.30 – 16.00 |

| | |
|---|---|
| 12-Juli-2025 | 09.30 – 16.00 |
| 19-Juli-2025 | 09.30 – 16.00 |

Dari jadwal tersebut maka koneksi antar kedua lokasi DC dan DRC akan aktif mulai pada jam 09.30 sampai dengan 16.00.

Penentuan jadwal koneksi data dan replikasi *server* di dasari oleh hasil uji coba melakukan replikasi *server* di saat jam kerja dan diluar jam kerja perusahaan. Berikut ini adalah grafik perbandingan traffic nya.




Gambar 4. Perbandingan penggunaan *Bandwidth* Uji Replikasi

Proses replikasi server menghasilkan beban *outbound* yang tinggi dan stabil dibandingkan *inbound* selama jam kerja. Tanpa replikasi, penggunaan *bandwidth* lebih ringan dan stabil karena hanya dipengaruhi aktivitas operasional harian. Replikasi di luar jam kerja efektif karena menghasilkan beban *outbound* tinggi tanpa mengganggu performa jaringan operasional.

Berikut adalah *log* hasil penjadwalan koneksi data pada tanggal 28 juni 2025 yang mana menunjukan bahwa koneksi jaringan antara *server* DC dan DRC berhasil terhubung pada jam 09.30 dan terputus secara otomatis pada jam 16.00.

Tabel 4. *Log Firewall* Hasil Penjadwalan Koneksi Data

| Tanggal | Waktu | Tipe Koneksi | Keterangan |
|---|---|---|---|
| 2025-06-28 | 09:30:02 | "vpn" | logdesc="Progress IPsec phase 2" msg="progress IPsec phase 2" action="negotiate" remip=103.129.152.58 locip=103.168.129.90 remport=500 locport=500 outintf="port1" cookies="9eea1bb99f7782df/90cbb903eda71271" user="103.129.152.58" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="VPN_TO_DR" status="success" init="local" mode="quick" dir="outbound" stage=1 role="initiator" result="OK" |
| 2025-06-28 | 09:30:02 | "vpn" | logdesc="IPsec SA installed" msg="install IPsec SA" action="install_sa" remip=103.129.152.58 locip=103.168.129.90 remport=500 locport=500 outintf="port1" cookies="9eea1bb99f7782df/90cbb903eda71271" user="103.129.152.58" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="VPN_TO_DR" role="initiator" in_spi="154caa02" out_spi="8be9059e" advpnsc=0 |
| 2025-06-28 | 16:00:02 | "vpn" | logdesc="IPsec phase 2 status changed" msg="IPsec phase 2 status change" action="phase2-down" remip=103.129.152.58 locip=103.168.129.90 remport=500 locport=500 outintf="port1" cookies="9eea1bb99f7782df/90cbb903eda71271" user="103.129.152.58" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="VPN_TO_DR" phase2_name="VPN_TO_DR" advpnsc=0 |
| 2025-06-28 | 16:00:02 | "vpn" | logdesc="Progress IPsec phase 2" msg="progress IPsec phase 2" action="Disconected" remip=103.129.152.58 locip=103.168.129.90 remport=500 locport=500 outintf="port1" cookies="9eea1bb99f7782df/90cbb903eda71271" user="103.129.152.58" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="VPN_TO_DR" status="success" init="local" mode="quick" dir="outbound" stage=2 role="initiator" result="D |

Berdasarkan log *firewall* Fortigate DC tanggal 28 Juni 2025, koneksi VPN antara DC dan DRC berhasil aktif secara otomatis pada pukul 09:30 melalui *tunnel* VPN_TO_DR dengan status sukses, menandakan koneksi siap digunakan untuk pertukaran data terenkripsi. Koneksi tersebut kemudian terputus secara normal pada pukul 16.00 karena masa aktif koneksi berakhir (IPsec SA *lifetime expired*), sehingga dapat disimpulkan bahwa uji coba penjadwalan koneksi data antara DC dan DRC berjalan dengan baik.

Berikut ini laporan hasil replikasi virtual *server* pada tanggal 28 juni 2025 sampai dengan 19 juli 2025.

Tabel 4. Laporan Hasil Replikasi *Server*

| Tanggal | Nama Server | Waktu Mulai Replikasi | Waktu Selesai Replikasi | Total Size | Size Transferred | Durasi | Status |
|---|---|---|---|---|---|---|---|
| 28-Jun-25 | RIF-AD | 09:56:07 | 10:06:21 | 160 GB | 366,6 MB | 0:10:14 | Sukses |
| | RIF-ANTIV | 10:01:01 | 10:49:02 | 200 GB | 2,1 GB | 0:48:01 | Sukses |
| | RIF-SERV01 | 11:32:51 | 14:23:40 | 3,1 TB | 3,3 GB | 2:50:49 | Sukses |
| | RIF-SERV03 | 10:15:22 | 11:38:25 | 500 GB | 2,4 GB | 1:23:03 | Sukses |
| | RIF-SERV05 | 10:30:31 | 12:19:58 | 500 GB | 5,7 GB | 1:49:27 | Sukses |
| 5-Jul-25 | RIF-AD | 09:45:39 | 10:00:00 | 160 GB | 1,5 GB | 0:14:21 | Sukses |
| | RIF-ANTIV | 10:00:03 | 11:30:54 | 200 GB | 10,1 GB | 1:30:21 | Sukses |
| | RIF-SERV01 | 11:30:29 | 15:52:37 | 3,1 TB | 7,9 GB | 4:22:08 | Sukses |
| | RIF-SERV03 | 10:15:30 | 12:40:33 | 500 GB | 6,2 GB | 2:25:03 | Sukses |
| | RIF-SERV05 | 10:31:48 | 14:02:06 | 500 GB | 12,2 GB | 3:30:18 | Sukses |
| 12-Jul-25 | RIF-AD | 09:45:32 | 09:55:50 | 160 GB | 581,5 MB | 0:10:18 | Sukses |
| | RIF-ANTIV | 10:00:33 | 10:31:50 | 200 GB | 914,3 MB | 0:31:17 | Sukses |
| | RIF-SERV01 | 11:30:30 | 14:56:00 | 3,1 TB | 4,9 GB | 3:25:30 | Sukses |
| | RIF-SERV03 | 10:15:28 | 11:38:16 | 500 GB | 2,2 GB | 1:22:48 | Sukses |
| | RIF-SERV05 | 10:30:09 | 12:29:46 | 500 GB | 4,7 GB | 1:59:37 | Sukses |
| 19-Jul-25 | RIF-AD | 09:54:56 | 10:13:48 | 160 GB | 2,1 GB | 0:18:52 | Sukses |
| | RIF-ANTIV | 10:00:21 | 10:40:59 | 200 GB | 2,3 GB | 0:40:38 | Sukses |
| | RIF-SERV01 | 11:56:44 | 15:44:14 | 3.1 TB | 4,9 GB | 3:47:30 | Sukses |
| | RIF-SERV03 | 10:15:20 | 11:57:17 | 500 GB | 2,9 GB | 1:41:57 | Sukses |
| | RIF-SERV05 | 12:56:18 | 13:34:29 | 500 GB | 1,9 GB | 0:38:11 | Sukses |

Laporan ini menyajikan hasil replikasi *server* antara *Data Center* (DC) dan *Disaster Recovery Center* (DRC) dilakukan secara mingguan pada lima *virtual server* menggunakan metode inkremental untuk menjaga ketersediaan data terkini. Seluruh proses replikasi selama periode pengujian berjalan berhasil tanpa gangguan, menunjukkan stabilitas sistem serta kesamaan data yang konsisten antara DC dan DRC.

Selama proses replikasi *server* berjalan telah terdeteksi beberapa gangguan yang terindikasi mencurigakan dari IP *address* DC 192.168.15.199 ke IP *address* DRC 192.168.14.22 melalui jalur VPN ke DRC namun telah berhasil di halau oleh sistem IPS (I*ntrution Prevention System*) *firewall*. Penulis menggunakan sampel *log* pada proses replikasi tanggal 28 juni 2025.

Tabel 4. Hasil *Log* Keamanan *Firewall* DC ke DRC Selama Replikasi

| Tanggal | Waktu | Sumber IP | Tujuan IP | Interface | Action | Info |
|---|---|---|---|---|---|---|
| 2025-06-28 | 12:43:55 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:43:20 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:42:45 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:42:10 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:41:35 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:41:00 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:40:24 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:39:49 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:39:14 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:38:39 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:38:04 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:37:29 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:36:54 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:36:19 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |
| 2025-06-28 | 12:35:43 | 192.168.15.199 | 192.168.14.22 | "VPN_TO_DR" | "dropped" | "Log4j & Malicious" |

Selama proses replikasi server, sistem *firewall* mendeteksi 14 upaya koneksi berbahaya dari jaringan internal DC menuju server DRC melalui jalur VPN dalam rentang waktu sekitar delapan menit. Seluruh aktivitas tersebut berhasil diblokir secara otomatis oleh mekanisme keamanan *firewall* dengan status *dropped*. Temuan ini mengindikasikan efektivitas *firewall* dalam mencegah potensi penyebaran *malware* dan akses ilegal ke sistem DRC selama proses replikasi.

### 3.3.4. Uji Coba *Disaster Recovery Plan* (DRP)

Skenario simulasi bencana dilakukan untuk menguji kesiapan sistem dalam mengalihkan operasi ke DRC. Dalam simulasi, seluruh *server* DRC diaktifkan dan pengguna mencoba mengakses seluruh sistem layanan penunjang operasional yang ada di DRC. Hasil uji coba sebagai berikut:

Tabel 5. Laporan Hasil Uji Coba DRP

| Aktivitas | Pelaksana | Waktu Mulai | Waktu Selesai | Durasi | Status |
|---|---|---|---|---|---|
| **Aktivasi Server (failover) DRC** | | | | | |
| Aktivasi VPN | Tim IT | 09:00:00 | 09:00:30 | 00:00:30 | Sukses |
| Mengakses Server DRC | Tim IT | 09:00:35 | 09:03:00 | 00:02:25 | Sukses |
| Aktivasi Virtual Server RIF-AD | Tim IT | 09:03:10 | 09:05:30 | 00:02:20 | Sukses |
| Aktivasi Virtual Server RIF-ANTIV | Tim IT | 09:05:35 | 09:07:55 | 00:02:20 | Sukses |
| Aktivasi Virtual Server RIF-SERV01 | Tim IT | 09:05:40 | 09:10:45 | 00:05:05 | Sukses |
| Aktivasi Virtual Server RIF-SERV03 | Tim IT | 09:05:45 | 09:08:30 | 00:02:45 | Sukses |
| Aktivasi Virtual Server RIF-SERV05 | Tim IT | 09:08:35 | 09:12:55 | 00:04:20 | Sukses |
| **Uji Coba Akses Sistem Layanan Operasional** | | | | | |
| Mengakses VPN | User | 09:15:00 | 09:15:30 | 00:00:30 | Sukses |
| Mengakses File Sharing | User | 09:15:35 | 09:15:40 | 00:00:05 | Sukses |
| Mengakses Sistem Aplikasi | User | 09:16:00 | 09:17:00 | 00:01:00 | Sukses |

Hasil Uji coba *failover* menunjukkan bahwa sistem DRC mampu mencapai RTO ±15 menit dengan RPO 7 hari, di mana data yang tersedia merupakan hasil sinkronisasi terakhir dari proses replikasi dan layanan utama dapat diakses dalam waktu singkat.

Hasil ini menunjukkan bahwa sistem DRC mampu menggantikan peran DC dalam waktu singkat, sehingga gangguan terhadap operasional dapat diminimalkan secara signifikan.

### 3.4. Perbandingan Sebelum dan Sesudah Implementasi

Keberhasilan dievaluasi secara komparatif sebelum dan sesudah implementasi.

Tabel 6. Perbandingan Sebelum dan Sesudah Implementasi

| Aspek | Sebelum Implementasi | Setelah Implementasi |
|---|---|---|
| Metode *Backup* | Manual (*copy-paste*) | Otomatis (Veeam + Penjadwalan koneksi) |
| Potensi Penyebaran *Virus* | Tinggi | Rendah (koneksi dibatasi) |
| Downtime Pemulihan *Server* | > 3 jam (Proses *restore* data *backup*) | < 15 menit |
| Risiko Kehilangan Data | Tinggi | Sangat Rendah |

### 3.5. Analisa dan Interpretasi Hasil

Bagian ini menganalisis hasil implementasi sistem backup dan replikasi virtual server dengan penjadwalan koneksi data pada DRC PT. XYZ Finance melalui perbandingan capaian pengujian terhadap tujuan penelitian serta evaluasi efektivitas dan efisiensi sistem yang diterapkan.

### 3.6. Ringkasan

Hasil penelitian menunjukkan bahwa penerapan sistem *backup* dan replikasi otomatis berbasis Veeam Backup & Replication dengan penjadwalan koneksi melalui *firewall* Fortigate secara signifikan meningkatkan keamanan, efisiensi jaringan, dan keandalan sistem dibandingkan metode manual sebelumnya. Sistem mampu mencapai kinerja Disaster Recovery Plan dengan RTO ±15 menit dan RPO 7 hari, serta meningkatkan kesiapan operasional perusahaan dalam menghadapi risiko TI berdasarkan perbandingan hasil uji coba DRP sebelum dan sesudah implementasi.

## 4. KESIMPULAN

Implementasi sistem backup dan replikasi virtual server berbasis Veeam Backup & Replication pada lingkungan virtualisasi VMware dengan penjadwalan koneksi melalui firewall Fortigate terbukti efektif menggantikan metode manual sebelumnya. Sistem ini meningkatkan keamanan jaringan dan efisiensi penggunaan bandwidth melalui pengaturan koneksi terjadwal, serta mampu mencapai kinerja Disaster Recovery Plan dengan RTO ±15 menit dan RPO 7 hari. Hasil evaluasi menunjukkan peningkatan signifikan pada keandalan backup, keamanan data, efisiensi jaringan, dan kesiapan operasional, sehingga seluruh tujuan penelitian dapat terpenuhi.

## 5. DAFTAR PUSTAKA

[1] E. Haryadi, dan Robi, S. Nusa Mandiri Jakarta, and K. Kunci---VMware, "Implementasi Sistem Backup Data Perusahaan Sebagai Bagian dari Disaster Recovery Plan Implementation of Corporate Data Backup Systems As Part of a Disaster Recovery Plan," 2019.

[2] N. Fitriawati, A. Herdiansah, R. Taufiq, and R. Destriana, "IT DISASTER RECOVERY PLAN DALAM MENDUKUNG BUSINESS CONTINUITY PLAN SAAT TERJADI FORCE MAJEURE," 2022.

[3] F. Adrianus and A. Setiyadi, "PEMBANGUNAN BACKUP, REPLIKASI DAN MONITORING SERVER SEBAGAI SOLUSI PENANGGULANGAN BENCANA PADA VIRTUALISASI SERVER DI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA BARAT," 2018.

[4] Y. Kusumo Sutojoyo, R. R. Saedudin, and B. Rahmat, "PERANCANGAN DISASTER RECOVERY PLAN UNTUK TEKNOLOGI DI PERUSAHAAN PT. XYZ," 2018.

[5] F. Faisal, "The backup recovery strategy selection to maintain the business continuity plan," *MATEC Web Conf.*, vol. 229, 2018, doi: 10.1051/matecconf/201822902001.

[6] W. A. Yuliono and A. Prihanto, "Sinergi Replikasi Server dan Sistem Failover pada Database Server untuk Mereduksi Downtime Disaster Recovery Planing (DRP)," *J. Informatics Comput. Sci.*, vol. 03, 2021.

[7] N. Sadikin and M. Sari, "REPLIKASI VIRTUAL MACHINE ANTARA DUA LOKASI TERPISAH UNTUK BACKUP DAN DISASTER RECOVERY," Jan. 2020.

[8] A. Nugraha and R. Amin, "Analisis Metode Replikasi Sistem Basis Data Di Pusintek Kementerian Keuangan," *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 6, no. 1, 2022, doi: 10.47970/siskom-kb.v6i1.329.

[9] T. B. Septiandoko, D. Desmulyati, and A. Taufik, "Implementasi Jaringan Internet Site To Site VPN Dengan Metode IPSec Pada PT Telkom Akses," *Comput. Sci.*, vol. 1, no. 1, pp. 18–26, 2021, doi: 10.31294/coscience.v1i1.138.

[10] D. Pupung, A. Politeknik, and N. Jakarta, "ANALISA INFRASTRUKTUR VIRTUALISASI DATA CENTER PADA PT TELKOMSEL UNTUK

MEMENUHI SERVICE AGREEMENT," May 2019.