

Strategi Disaster Recovery dengan Virtualisasi: Backup dan Restore Sistem Operasi di VMware dengan Menggunakan Snapshot

Rakhmadi Rahman, Anugrah Dwi Ansarna, Eka Tanduklangi

Program Studi Sistem Informasi, Institut Teknologi Bacharuddin Jusuf Habibie, Indonesia

ugapares01@gmail.com, ekalangi96@gmail.com

Korespondensi penulis: ugapares01@gmail.com

Abstract: A Disaster Recovery Plan (DRP) is a structured approach that describes how an organization can carry out its operations after an unplanned incident that can result in system failure. Creating strong system resilience requires an IT team with strong experience and understanding as well, and this is the background of this research. This research aims to provide practical guidance in implementing disaster recovery strategies with virtualization, especially the snapshot feature on VMware Workstation to test disaster scenarios and evaluate their recovery effectiveness.

Keywords: *Disaster Recovery, Virtualisasi, VMware, Snapshot.*

Abstrak: Disaster Recovery Plan (DRP) adalah pendekatan terstruktur yang menggambarkan bagaimana suatu organisasi dapat menjalankan operasinya setelah terjadi insiden yang tidak terencana yang dapat mengakibatkan kegagalan pada sistem. Untuk membuat ketahanan sistem yang kuat, dibutuhkan tim IT yang memiliki pengalaman dan pemahaman yang kuat juga dan inilah yang menjadi latar belakang penelitian ini. Penelitian ini bertujuan untuk memberikan panduan praktis dalam mengimplementasikan strategi disaster recovery dengan virtualisasi khususnya fitur snapshot pada VMware Workstation untuk menguji skenario bencana dan mengevaluasi efektivitas pemulihannya.

Kata kunci: Pemulihan Bencana, Virtualisasi, VMware, Snapshot.

1. PENDAHULUAN

Dalam era Society 5.0 ini berkembangnya jaringan komputer dan teknologi informasi telah menjadi tulang punggung operasional di seluruh dunia. Kecepatan akses informasi dan kemampuan untuk bekerja secara kolaboratif sangat mempengaruhi efisiensi dan produktivitas. Ketergantungan tersebut meningkatkan resiko gangguan sistem akibat bencana alam, kesalahan manusia, kegagalan hardware, maupun serangan cyber. oleh karena itu, Disaster Recovery Plan (DRP) menjadi sangat penting untuk memastikan kontinuitas operasional tetap aman. Terdapat 5 tipe DRP yaitu Virtualized Disaster Recovery Plan, Network Disaster Recovery Plan, Cloud Disaster Recovery Plan, Data Center Disaster Recovery Plan, dan DRaaS (Disaster Recovery as a Client Service) (Andrianto & Setiawan, 2021)

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam hal pengelolaan data dan sistem informasi. Salah satu aspek penting dalam manajemen data adalah strategi pemulihan bencana (disaster recovery) (Patrao, 2024). Strategi ini bertujuan untuk memastikan keberlangsungan

operasional dan ketersediaan data meskipun terjadi gangguan atau bencana yang tidak terduga. Virtualisasi menjadi salah satu teknologi kunci yang digunakan dalam strategi disaster recovery modern.

VMware, sebagai salah satu penyedia solusi virtualisasi terkemuka, menawarkan berbagai fitur yang dapat membantu dalam proses backup dan restore sistem operasi. Salah satu fitur andalan VMware adalah snapshot, yang memungkinkan pengguna untuk mengambil gambar kondisi sistem operasi pada titik waktu tertentu. Snapshot ini dapat digunakan untuk mengembalikan sistem operasi ke kondisi sebelumnya dengan cepat dan efisien, sehingga meminimalkan waktu downtime dan kerugian data (Wibowo & Utomo, 2022)

Penelitian ini membahas tentang penerapan Disaster Recovery menggunakan teknologi virtualisasi (Virtualized Disaster Recovery Plan), Teknologi virtualisasi, khususnya VMware, menawarkan solusi yang efektif untuk DR melalui fitur snapshot yang memungkinkan pembuatan salinan dari keadaan sistem pada waktu tertentu. Melalui snapshot, tim IT dapat dengan mudah mensimulasikan berbagai skenario bencana tanpa risiko kerusakan permanen pada sistem operasional, memungkinkan mereka untuk mempraktikkan dan memahami langkah-langkah pemulihan secara langsung. Selain itu, snapshot menyediakan cara yang cepat dan efisien untuk mengembalikan sistem ke keadaan sebelumnya, sehingga tim IT dapat mengevaluasi dan mengasah kemampuan mereka dalam mengelola situasi darurat, mengidentifikasi potensi masalah, dan menerapkan perbaikan yang diperlukan.

2. METODE PENELITIAN

Penelitian ini menggunakan metode Agile dalam pengembangan strategi DR. Metode ini dipilih karena fleksibilitasnya dalam menyesuaikan diri dengan perubahan yang cepat. Tahapan dalam metode Agile meliputi perencanaan, pengujian berkala, pengembangan iteratif, evaluasi, dan penyesuaian. Tools yang digunakan dalam penelitian ini termasuk Media Creation Tool dan ISO Windows 10 untuk menyiapkan lingkungan pengujian.

3. HASIL DAN PEMBAHASAN

Snapshot adalah fitur yang sangat berguna dalam konteks Disaster Recovery (DR) karena menawarkan sejumlah keunggulan yang signifikan dibandingkan metode pemulihan lainnya. Pertama, snapshot memungkinkan pembuatan cadangan lengkap dari sistem pada titik waktu tertentu. Ini berarti bahwa jika terjadi bencana, sistem dapat dikembalikan ke

kondisi terakhir yang diketahui baik dalam hitungan menit, mengurangi waktu pemulihan secara drastis. Perbandingan snapshot dengan backup tradisional

Aspek	Snapshot	Backup Tradisional
Kecepatan Pengambilan	Sangat cepat (hampir instan)	Lebih lambat
Penggunaan Penyimpanan	Hemat ruang (hanya menyimpan perubahan)	Membutuhkan lebih banyak ruang
Seberapa Sering Bisa Dilakukan	Bisa sering (setiap menit atau jam)	Biasanya harian atau mingguan
Kecepatan Pemulihan	Cepat dan mudah	Bisa lebih lambat
Ketegantungan Sistem	Tergantung pada sistem asli	Disimpan terpisah dari sistem asli
Penyimpanan Jangka Panjang	Tidak cocok untuk jangka panjang	Sangat cocok
Keamanan	Aman jika sistem asli aman	Lebih aman (bisa disimpan di lokasi terpisah dan dienkripsi)
Kemudahan Pengelolaan	Mudah dikelola	Lebih rumit

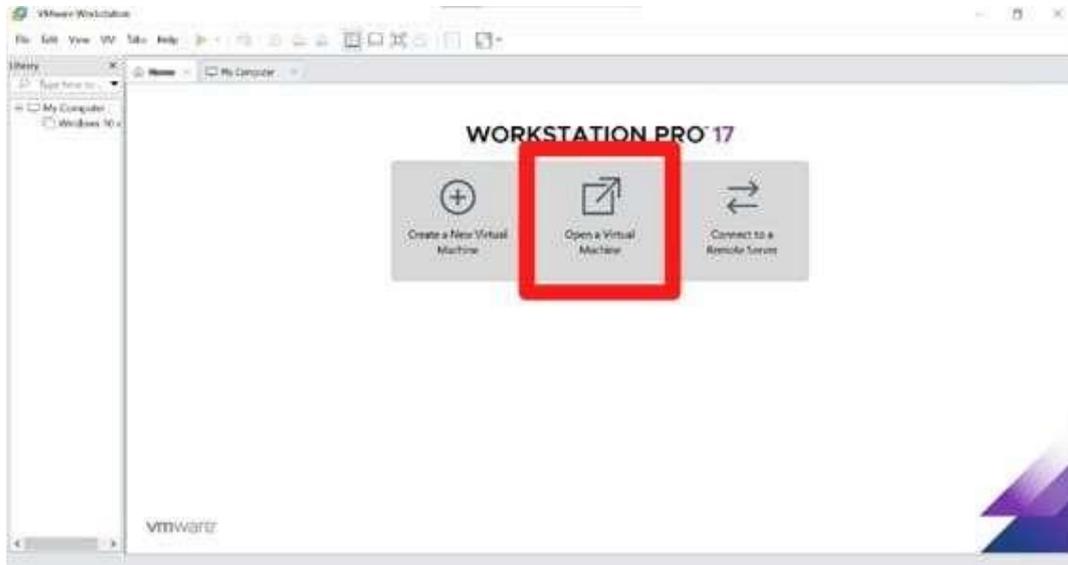
Gambar 3.1 Perbandingan Snapshot dengan Backup Tradisional

Tahap pertama dalam implementasi adalah menginstall dan mengonfigurasi VMware workstation.



Gambar 3.2 VMware Workstation Pro Setup

Setelah VMware terinstall dan dikonfigurasi, langkah selanjutnya adalah membuat dan konfigurasi virtual machine.



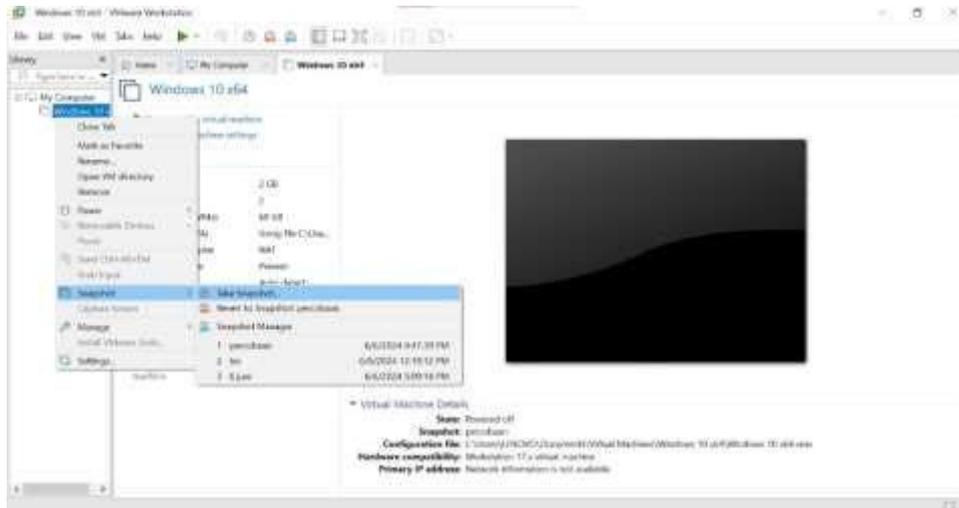
Gambar 3.3 Virtual Machines (VMs)



Gambar 3.4 New Virtual Machine Wizard

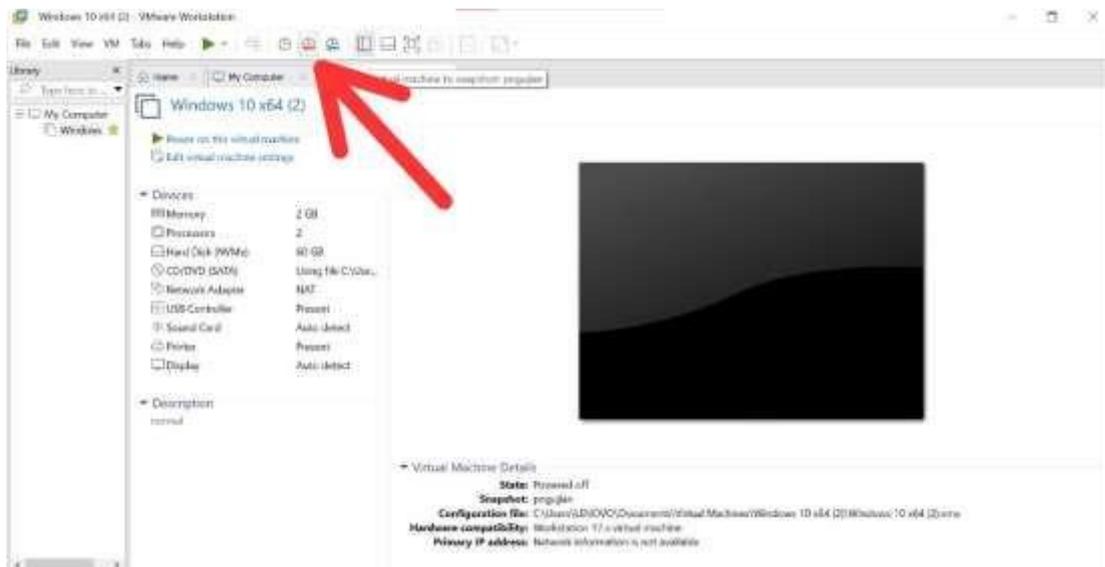
Tahap selanjutnya adalah pengambilan snapshot pada virtual machine yang telah dibuat. Snapshot berfungsi sebagai titik pemulihan, memungkinkan sistem dikembalikan ke kondisi yang telah ditentukan.

Setelah melakukan tahapan berikut, lingkungan untuk latihan pemulihan dan simulasi bencana seperti kerusakan sistem, kehilangan data, dan serangan siber dapat dilakukan untuk menguji keefektifan sistem yang diterapkan.



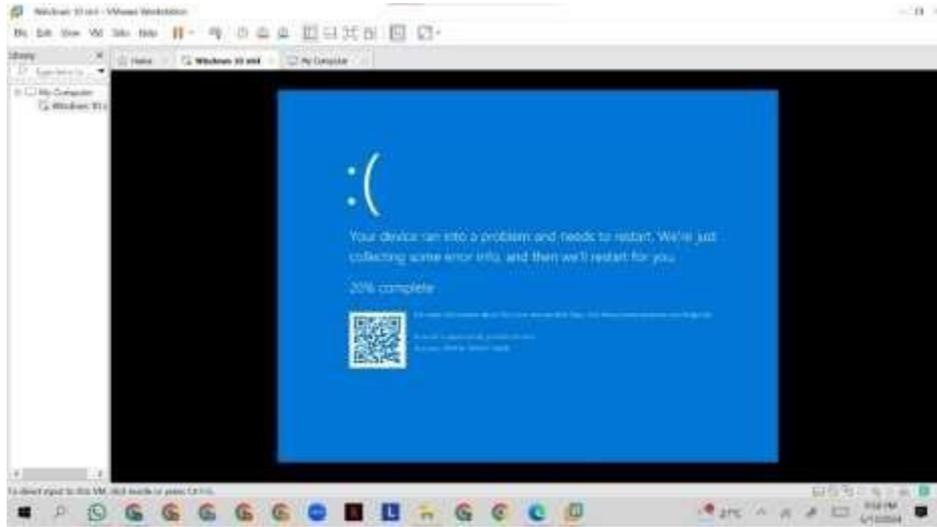
Gambar 3.5 Snapshot

Untuk melakukan rollback pada virtual machine yang telah rusak caranya klik kanan pada virtual machine dan pilih titik snapshot yang telah dibuat.



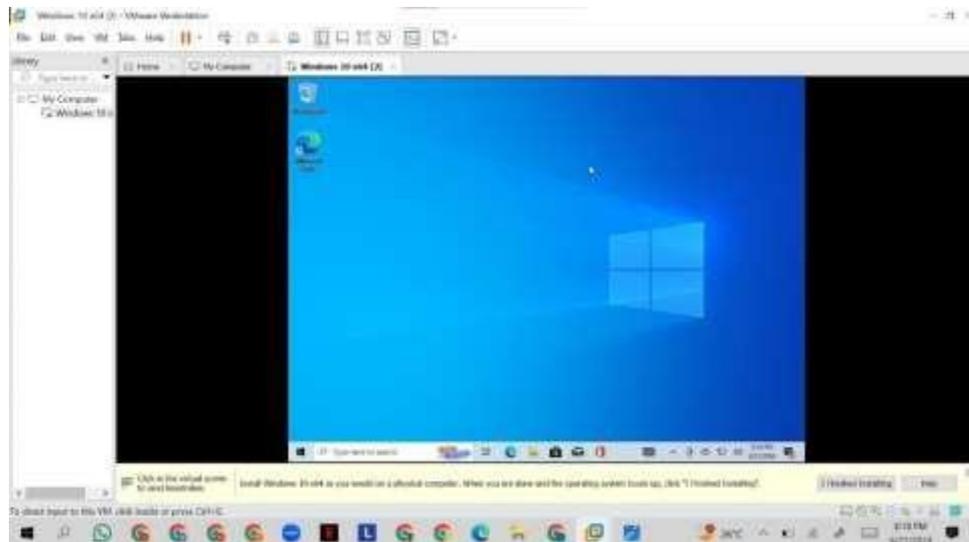
Gambar 3.6 Rollback pada Snapshot

Contoh Simulasi Bencana



Gambar 3.7 Simulasi Bencana

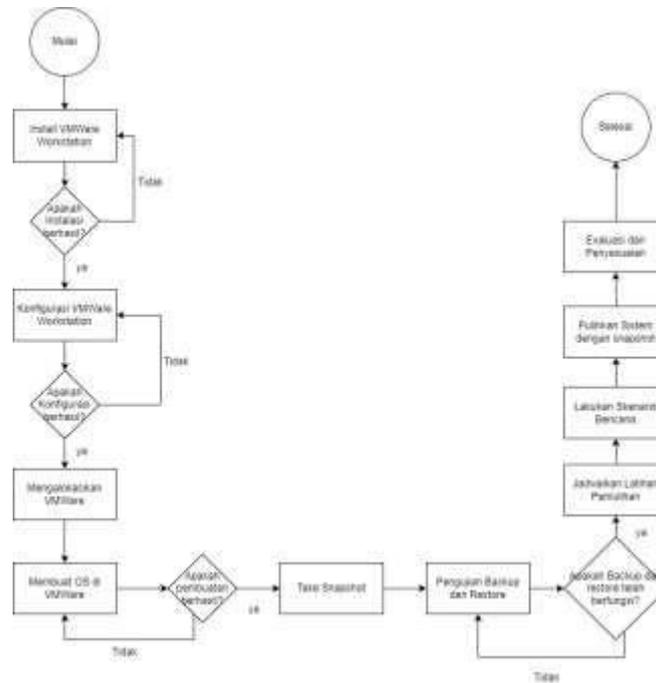
Pada gambar di atas, terdapat kerusakan sistem akibat malware yang merusak file "System32". dengan fitur snapshot, sistem dapat dipulihkan dengan beberapa klik saja.



Gambar 3.8 Sesudah Skenario Bencana

Dengan melakukan latihan pemulihan yang terjadwal dan simulasi bencana yang teliti, organisasi dapat memperkuat kesiapannya dalam menghadapi risiko serta meningkatkan kemampuan untuk pulih dengan cepat dari gangguan yang mungkin terjadi. Dengan pendekatan ini, diharapkan organisasi dapat meningkatkan ketahanan sistem mereka

dan memastikan bahwa mereka siap menghadapi berbagai ancaman atau gangguan yang mungkin terjadi. Berikut flow chart dari tahap implementasi penggunaan VMWare:



Gambar 3.9 Tahapan Implementasi

a. Backup Data Skala Besar

Untuk melakukan backup data berukuran besar yang bukan dalam cakupan snapshot, Google Cloud Platform (GCP) adalah pilihan yang bagus karena dapat menangani volume data besar dengan efisien. Berikut langkah-langkahnya dari proses backup sampai pemulihan data:

- 1) Pilih Layanan: Pertama, pilih layanan di Google Cloud yang cocok untuk menyimpan data Anda. Misalnya, Google Cloud Storage untuk menyimpan data dalam bentuk file atau Google Compute Engine untuk mengelola mesin virtual.
- 2) Siapkan Data: Pastikan data yang ingin Anda backup sudah disiapkan dengan baik. Pastikan data terstruktur dengan benar dan siap untuk disimpan di cloud.
- 3) Kirim Data: Untuk mengirim data ke Google Cloud, Anda bisa menggunakan layanan seperti Google Cloud Storage Transfer Service untuk transfer data otomatis atau menggunakan alat fisik seperti Google Cloud Storage Transfer Appliance untuk data dalam skala besar.

- 4) Simpan dan Kelola: Setelah data terunggah ke Google Cloud Storage, Anda bisa mengatur data tersebut dengan mudah. Gunakan fitur seperti manajemen siklus hidup untuk mengelola data secara otomatis, termasuk penghapusan atau pemindahan data ke tempat penyimpanan yang lebih murah.
- 5) Backup Rutin: Tetapkan jadwal backup data secara teratur. Google Cloud menyediakan alat dan API untuk membuat backup otomatis dan mengatur berapa lama data akan disimpan.
- 6) Pulihkan Data: Jika terjadi kehilangan data, Anda bisa memulihkan data dengan mudah menggunakan snapshot atau backup yang sudah tersimpan di Google Cloud Storage. Proses ini bisa dilakukan dengan mudah melalui antarmuka pengguna Google Cloud atau menggunakan perintah API.
- 7) Keandalan dan Keamanan: Google Cloud menawarkan infrastruktur global yang aman dan terpercaya. Data backup Anda disimpan di berbagai lokasi untuk memastikan ketersediaan dan keamanan yang maksimal.

Dengan menggunakan Google Cloud untuk backup data berukuran besar, Anda mendapatkan keuntungan dari infrastruktur kuat dan layanan yang dirancang untuk mengelola data besar dengan efisien. Ini akan membantu memastikan bahwa data perusahaan Anda tetap aman, dapat dipulihkan dengan cepat, dan selalu tersedia ketika Anda membutuhkannya.

4. KESIMPULAN DAN SARAN

Virtualisasi dan fitur snapshot di VMware merupakan solusi yang efektif untuk strategi disaster recovery. Dengan pendekatan ini, organisasi dapat meningkatkan ketahanan sistem informasi mereka dan memastikan pemulihan yang cepat saat terjadi bencana. Penelitian ini juga menggarisbawahi pentingnya pelatihan rutin, peningkatan infrastruktur, dan evaluasi berkelanjutan untuk memastikan kesiapan sistem menghadapi berbagai ancaman.

Beberapa saran yang dapat diberikan untuk penelitian selanjutnya dan peningkatan efektivitas strategi ini meliputi:

- a. Mengadakan pelatihan rutin untuk staf IT tentang prosedur DR.
- b. Meningkatkan infrastruktur hardware dan jaringan yang mendukung VMware.
- c. Melakukan evaluasi dan pembaruan strategi DR secara berkala.
- d. Meneliti perbandingan antara berbagai platform virtualisasi untuk menentukan yang paling efektif dalam skenario DR

DAFTAR PUSTAKA

- Andrianto, A., & Setiawan, H. (2021). "Penerapan Virtualisasi pada Disaster Recovery di Perusahaan Jasa Keuangan," *Jurnal Teknologi Informasi dan Komunikasi*, 10(1), 45-55.
- Khaled Elgdamsi, M. E. (n.d.). *Implementing a Disaster Recovery Solution for Datacenters Using VMware Site Recovery Manager*.
- Patrão, L. (2024). *vSphere Backup and Disaster Recovery*.
- Seemab Hameed, MS (2021). RENCANA PEMULIHAN OTONOMI DENGAN VIRTUALISASI SERVER.
- Wibowo, B., & Utomo, S. (2022). "Optimalisasi Backup dan Restore dengan VMware Snapshot pada Sistem Perbankan," *Jurnal Sistem Informasi*, 14(2), 89-102