IMPLEMENTASI BACKUP SOLUTION BERBASIS CLOUD UNTUK MENDUKUNG KEANDALAN VPN SERVER PADA PT WEEFER INDONESIA

Andi, Gautama Wijaya, Haeruddin
Email korespondensi: 2132065.andi@uib.edu, gautama@uib.edu, haeruddin@uib.edu

Abstrak

Data merupakan salah satu asset yang paling berharga dalam perusahaan. Data-data tersebut perlu dikelola dengan baik untuk mendukung kegiatan operasi sehari-hari. Salah satu langkah strategis yang dapat dilakukan untuk menjaga data tersebut adalah dengan menyiapkan cadangan data untuk memitigasi terjadinya bencana. Dengan berdasar pada observasi yang telah dilakukan, artikel ini bertujuan untuk mengimplementasi solusi *backup* pada salah satu perusahaan IT, PT. Weefer Indonesia, terutama pada server VPN yang digunakannya. Hasil dari penelitian menunjukkan bahwa implementasi solusi *backup* telah berjalan dengan baik, dan *file* yang di-*backup* dapat direstorasi tanpa adanya modifikasi.

Kata Kunci: *Backup, VPN, AnyBackup, Huawei Cloud*

Abstract

Data is one of the most valuable assets in a company. These data need to be managed properly to support daily operations. One strategic step that can be taken to protect the data is to prepare a data backup to mitigate disasters. Based on the observations that have been made, this article aims to implement backup solution at an IT company, PT. Weefer Indonesia, especially on their VPN server. The result of this study showed that the implementation of the backup solution was successful, and the backed-up file can be restored without any modifications.

Keywords: *Backup, VPN, AnyBackup, Huawei Cloud*

Pendahuluan

Dalam era digital yang semakin berkembang pesat, data telah menjadi salah satu aset yang paling berharga bagi perusahaan (Haryadi et al., 2019). Data-data tersebut perlu dikelola dengan baik untuk mendukung kegiatan operasi sehari-hari, dan sekaligus sebagai landasan dalam pengambilan keputusan strategis.

Berdasarkan riset pada tahun 2020 (Mendonça et al., 2020), perusahaan-perusahaan seperti Google, AWS (Amazon Web Services), Facebook, dan bank HSBC pernah mengalami gangguan yang memengaruhi layanan mereka dan menyebabkan gangguan di seluruh dunia. Hal ini menunjukkan bahwa terlepas dari ukuran perusahan atau target pasarnya, semuanya rentan terhadap peristiwa bencana.

Implementasi sistem *backup* yang efektif merupakan salah satu langkah kritis untuk memastikan bahwa data perusahaan tetap aman dan dapat dipulihkan dalam kondisi darurat. Gangguan teknis, kesalahan manusia (*human error*), serangan siber, dan bencana alam dapat menjadi ancaman yang mengakibatkan terjadinya kehilangan data (Plaka, 2022; Tatineni, 2023; Yuliono & Prihanto, 2021). Tanpa adanya implementasi strategi backup, perusahaan berisiko mengalami kerugian finansial yang signifikan, kerusakan reputasi, dan gangguan operasional yang parah (Tatineni, 2023).

Masalah

PT. Weefer Indonesia adalah salah satu pionir dalam dunia IT yang menyediakan solusi IT dengan tujuan untuk menghadirkan produk atau servis yang efektif dan ditingkatkan kepada para pelanggannya (Weefer, 2024). Dalam pengoperasiannya, PT. Weefer Indonesia menggunakan *Virtual Private Network* untuk menfasilitasi para karyawan dalam pekerjaan *remote control*. VPN tersebut terinstal dalam sebuah server yang berada pada kantor mereka. Berdasarkan observasi telah dilakukan, VPN server tersebut terpantau masih belum dicadangkan.

Dengan menyadari pentingnya *backup*, artikel ini membahas implementasi sistem *backup* pada server VPN di PT. Weefer Indonesia. Tujuan dari artikel ini adalah untuk menerapkan solusi *backup* pada VPN server di PT. Weefer Indonesia.

Metode

Implementasi *backup* dilakukan melalui beberapa tahapan sebagai berikut:

1. Tahap observasi, yaitu tahap pengamatan server dan jaringan kantor PT. Weefer Indonesia.
2. Tahap persiapan, yaitu tahap analisis dan perancangan solusi *backup* untuk VPN server di PT. Weefer Indonesia.
3. Tahap pelaksanaan, yaitu tahap implementasi solusi *backup* yang telah dirancang pada VPN server di PT. Weefer Indonesia.

4. Tahap evaluasi, yaitu tahap verifikasi solusi *backup* yang telah dirancang pada VPN server di PT. Weefer Indonesia

Implementasi tersebut dilakukan dengan jadwal pelaksanaan sebagai berikut:

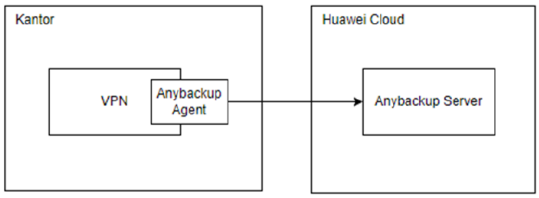
Tabel 1. Jadwal Pelaksanaan Kegiatan PkM

No	Kegiatan	Sep	Okt	Nov	Des
1	Observasi Jaringan Kantor Mitra	✓			
2	Penentuan *tools* yang digunakan untuk perancangan solusi *backup*	✓			
3	Pembiasaan fitur-fitur dalam *tools* yang digunakan untuk perancangan solusi *backup*		✓		
4	Perancangan dan implementasi solusi *backup*			✓	✓
5	Penyerahan luaran kepada mitra dan penilaian hasil luaran oleh mitra				✓

Pembahasan

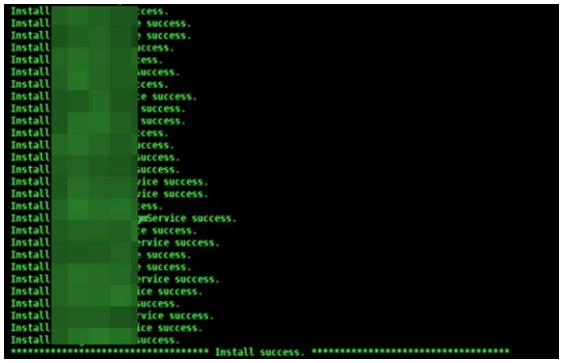
Tahap observasi dilakukan dengan menganalisis jaringan lokal kantor Weefer dan memahami struktur jaringan yang telah dibangun pada kantor tersebut.

Setelah dilakukan observasi, tahap persiapan dimulai dengan memilih dan merancang solusi *backup* sesuai dengan kebutuhan perusahaan. Dalam implementasi ini, solusi *backup* yang diterapkan adalah solusi *backup* ke Huawei Cloud dengan menggunakan *tools* AnyBackup.

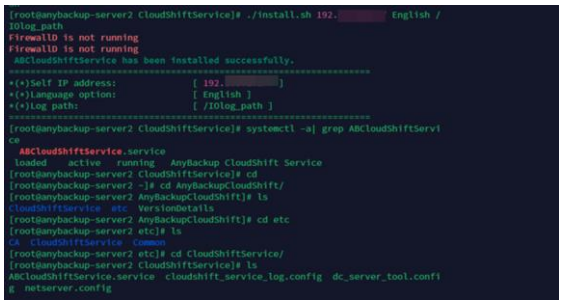


Gambar 1. Arsitektur Implementasi

Tahap pelaksanaan dimulai dengan melakukan instalasi *tools* AnyBackup beserta paket tambahannya pada sebuah server VM (*Elastic Cloud Server*) di Huawei Cloud.

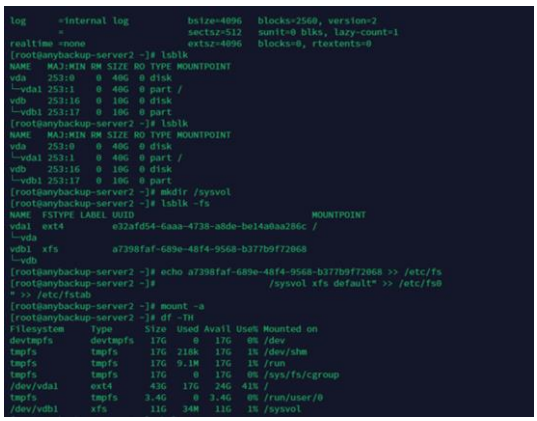


Gambar 2. Instalasi *tools* AnyBackup pada ECS Huawei Cloud



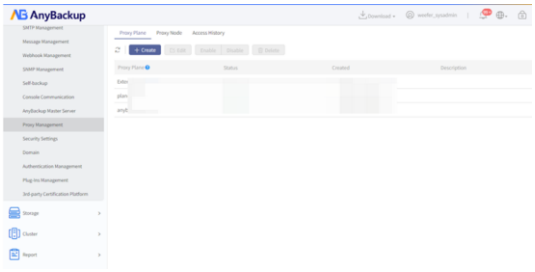
Gambar 3. Instalasi Paket Tambahan *tools* AnyBackup

Setelah instalasi selesai, dilakukan *setup* pada *storage* server tersebut untuk dijadikan sebagai tempat penyimpanan *metadata backup*. *Setup* tersebut dilakukan dengan menyiapkan partisi pada *storage*, memuat *file system* dari partisi tersebut, dan *mount file system* tersebut pada *path* tertentu.

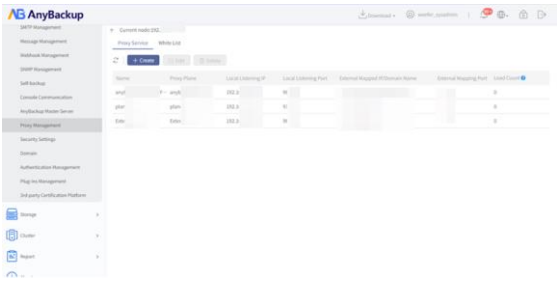


Gambar 4. Partisi Server

Sistem *backup* ini akan diakses melalui internet secara publik. Untuk mendukung hal tersebut, dilakukan penyetelan *proxy* dan *port* yang dapat digunakan untuk berkomunikasi dengan *tools* tersebut.



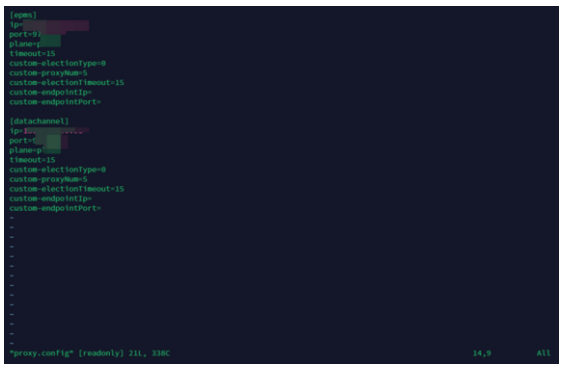
Gambar 5. Penyetelan *Proxy*



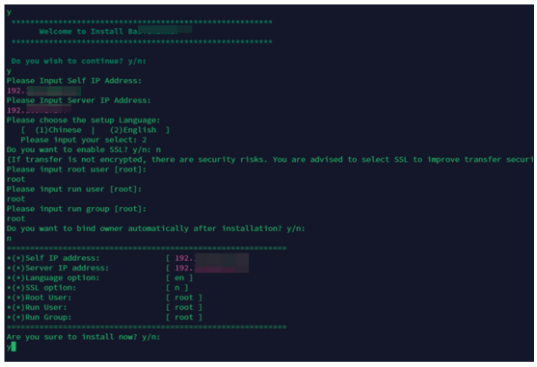
Gambar 6. Penyetelan *Port*

Setelah seluruh persiapan pada server AnyBackup, dilakukan instalasi *agent* pada server VPN kantor PT. Weefer Indonesia. Proses instalasi tersebut dapat dipecah menjadi beberapa tahapan, di antaranya proses *depackaging*, penyetelan *proxy*, dan instalasi *agent*.

Gambar 7. *File Depackaging* pada Server VPN

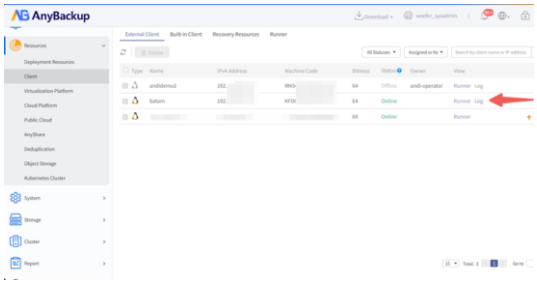


Gambar 8. Penyetelan *Proxy* pada Server VPN



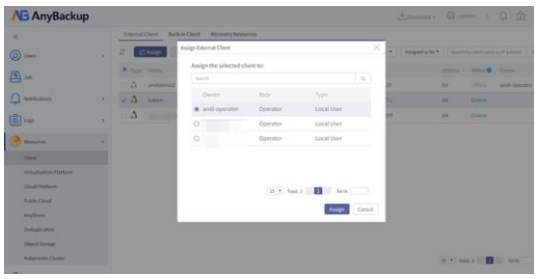
Gambar 9. Instalasi *Agent* pada Server VPN

Setelah *agent* berhasil terinstal pada server VPN, dilakukan verifikasi keberhasilan tersebut dengan mengecek konsol AnyBackup. Hasil menunjukkan bahwa server VPN tersebut telah terdeteksi dan dapat dilakukan *backup*.



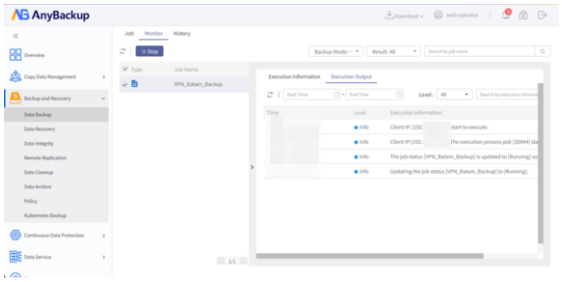
Gambar 10. Server VPN Terdeteksi

Untuk dapat melakukan *backup* terhadap server VPN, dilakukan pembuatan akun pada AnyBackup dan pemberian akses *backup* server VPN kepada akun tersebut.

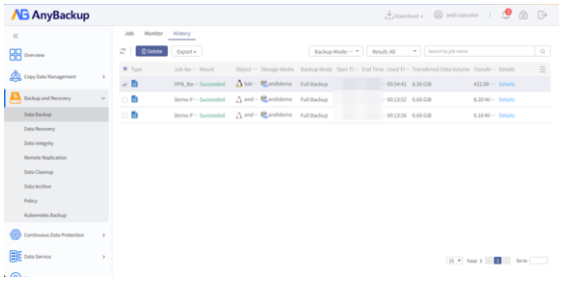


Gambar 11. Pemberian Akses *Backup*

Setelah mendapatkan akses *backup*, proses *backup* dilakukan dengan penambahan *backup job* pada konsol AnyBackup. Tipe *backup* yang dipilih adalah *file backup*, dengan tujuan apabila *file* konfigurasi atau *file* akses VPN terjadi masalah, maka pihak yang bersangkutan dapat melakukan restorasi *file* dengan cepat menggunakan AnyBackup.



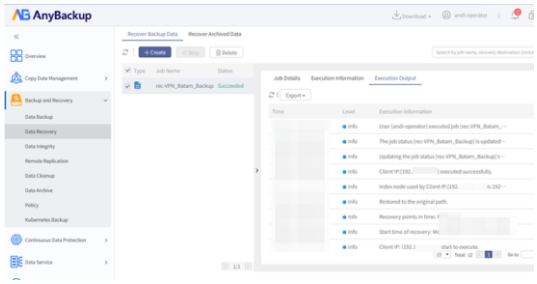
Gambar 12. Proses *Backup*



Gambar 13. *Backup* Berhasil

Tahap evaluasi dilakukan dengan pengetesan hasil *backup* yang telah dilakukan dengan percobaan restorasi. Percobaan tersebut dilakukan dengan menghapus salah satu *file* VPN *client* pada server VPN, kemudian melakukan restorasi *file*. Verifikasi *file* dilakukan dengan membandingkan hasil SHA256SUM pada *file* sebelum dihapus dan *file* yang telah direstorasi.

Gambar 14. Proses Penghapusan *File* VPN *Client*



Gambar 15. Proses Restorasi

Gambar 16. Hasil Setelah Restorasi

Hasil menunjukkan bahwa *file* VPN *client* sebelum dihapus dan setelah restorasi memiliki nilai SHA256SUM yang sama. Hal ini mengindikasikan bahwa tidak terjadinya perubahan pada *file* yang direstorasi, sehingga proses *backup* dan restorasi yang dilakukan telah berjalan dengan baik.

Simpulan

PT. Weefer Indonesia merupakan sebuah perusahaan yang bergerak di bidang teknologi. Dalam observasi yang telah dilakukan, VPN server di kantor PT. Weefer Indonesia masih belum memiliki *backup*. Dengan menyadari pentingnya *backup* tersebut, pada artikel ini dirancang dan diimplementasikan solusi *backup* dengan menggunakan AnyBackup ke Huawei Coud. Hasil dari implementasi ini menunjukkan bahwa solusi *backup* yang diterapkan pada perusahaan dapat berjalan dengan lancar, dan terbukti dapat merestorasi *file-file* pada server VPN tanpa adanya modifikasi pada *file* tersebut.

Adapun beberapa kekurangan dan saran dari proyek yang telah dilaksanakan ini, di antaranya:

1. Proyek ini masih belum mencakup *backup policy* untuk server VPN. Proyek selanjutnya dapat menganalisa kebutuhan perusahaan untuk menerapkan *policy* tersebut.
2. Proyek ini tidak mencakup keamanan data *backup*, baik *in transit*, maupun *in rest*, sehingga alangkah baiknya proyek kedepannya dapat mengimplementasi *encryption* ataupun *tunneling* untuk menjamin keamanan data *backup* ini.

Daftar Pustaka

Haryadi, E., Abdussomad, & Robi. (2019). Implementasi Sistem Backup Data Perusahaan Sebagai Bagian dari Disaster Recovery Plan Implementation of Corporate Data Backup Systems As Part of a Disaster Recovery Plan. *Sainstech*, *6*(2), 1410–7104.

Mendonça, J., Lima, R., & Andrade, E. (2020). Evaluating and modelling solutions for disaster recovery. *International Journal of Grid and Utility Computing*, *11*(5), 705–713. https://doi.org/10.1504/IJGUC.2020.110049

Plaka, R. (2022). *Backup & Data Recovery in Cloud Computing:*

A Systematic Mapping Study. 94–113.

Tatineni, S. (2023). Cloud-Based Business Continuity and Disaster Recovery Strategies. *International Research Journal of Modernization in Engineering Technology and Science*, *November*. https://doi.org/10.56726/irjmets46236

Weefer. (2024). *About Weefer*. https://www.weefer.co.id/about-us/

Yuliono, W. A., & Prihanto, A. (2021). Sinergi Replikasi Server dan Sistem Failover pada Database Server untuk Mereduksi Downtime Disaster Recovery Planing (DRP). *Journal of Informatics and Computer Science (JINACS)*, *3*(01), 29–38. https://doi.org/10.26740/jinacs.v3n01.p29-38