JURNAL DEVICE, VOL. 14 NO 2, November 2024, 236-242
ISSN: 0216-9185 | eISSN: 2746-8984

# IMPLEMENTASI *UNTRUSTED HYBRID ACTIVE DIRECTORY* DAN OPTIMALISASI AKUN PENGGUNA *MICROSOFT* ENTRA ID SEBAGAI *SSO (SINGLE SIGN-ON)*

**Edy Yuliansyah [1)], Fezan Nabawi [2)], Andi Aljabar [3)]**

*[1) 2) 3)] Program Studi Teknik Informatika, Universitas Nahdlatul Ulama Indonesia*
*Jakarta, Indonesia*
*edyyuliansyah@unusia.ac.id [1)], fezan@unusia.ac.id [2)], andialjabar@unusia.ac.id [3)]*

## ABSTRAK

PT X merupakan salah satu Perusahaan farmasi terbesar di Indonesia saat ini memiliki sebanyak 42 BU (Bisnis Unit), di mana 10 BU diantaranya per 2024 tercatat memiliki 3.372 *user* aktif yang secara manajemennya masih tergabung dalam AD (*Active Directory*) *On-premise server* yang sepenuhnya dikelola oleh *Corporate* IT. Secara umum kondisi tersebut memang efisien, namun di sisi lain fleksibilitas seluruh entitas dalam mengelola *user* dan perangkat miliknya dalam AD terbatas, karena seluruh entitas mengikuti policy yang telah ditentukan oleh *Corporate IT*. Terdapat pula potensi penyalahgunaan akses, karena tiap entitas hanya dipisahkan pada level OU (*Organitation Unit*), artinya secara tidak langsung antar entitas bisa saling berkomunikasi karena berada di *Forest Domain* yang sama, dampak besarnya jika *server* AD tersebut bermasalah. Tujuan dari penelitian ini adalah memastikan tiap entitas dapat melakukan manajemen *user* dan computer nya masing-masing, dengan memanfaatkan akun *Microsoft* EntraID (atau sebelumnya disebut juga *Microsoft* AD Azure) untuk otentikasi *Single Sign-On* untuk *login* komputer, *email* dan jaringan. Hasil yang diharapkan dari penelitian ini ialah berupa skema manajemen *Active Directory* yang efisien secara biaya, sederhana dalam operasional, fleksibel dalam pengelolaan, dan *agile* terhadap kemajuan teknologi.

Kata Kunci : *Active Directory, Microsoft, AD Azure, EntraID, Domain,* PPDIOO

## *ABSTRACT*

*PT X is one of the largest pharmaceutical companies in Indonesia currently has 42 BU (Business Units), where 10 BUs as of 2024 were recorded as having 3,372 active users whose management is still included in the AD (Active Directory) On-premise server which is fully managed by Corporate IT. In general, this condition is efficient, but on the other hand, the flexibility of all entities in managing their users and devices in AD is limited, because all entities follow the policies determined by Corporate IT. There is also the potential for misuse of access, because each entity is only separated at the OU (Organization Unit) level, meaning that indirectly between entities can communicate with each other because they are in the same Forest Domain, the big impact if the AD server has problems. The purpose of this study is to ensure that each entity can manage its own users and computers, by utilizing a Microsoft EntraID account (or previously known as Microsoft AD Azure) for Single Sign-On authentication for computer logins, email and networks. The expected results of this study are in the form of an Active Directory management scheme that is cost efficient, simple in operation, flexible in management, and agile towards technological advances.*

*Keywords: Active Directory, Microsoft, AD Azure, EntraID, Domain,* PPDIOO

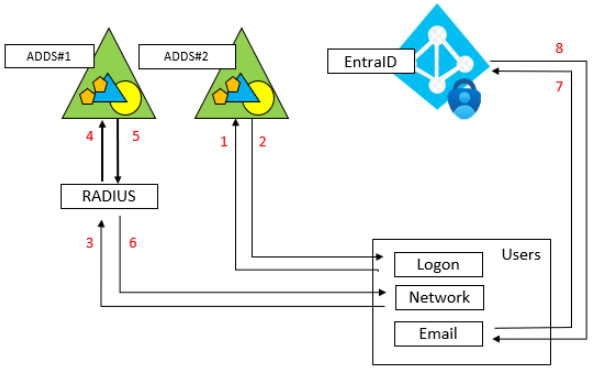
## 1. PENDAHULUAN

PT X merupakan salah satu Perusahaan farmasi terbesar di Indonesia yang saat ini memiliki sebanyak 42 BU (Bisnis Unit) yang tersebar di banyak kota di Indonesia dan negara lainnya, di mana 10 BU diantaranya per 2024 tercatat memiliki 3.372 *user* aktif yang secara manajemennya masih tergabung dalam AD (*Active Directory*) *On-premise server* yang sepenuhnya dikelola oleh *Corporate* IT. AD sendiri berfungsi sebagai otentikasi *user* dengan otoritas terpusat pada jaringan komputer terhadap keamanan jaringan, verifikasi akses *user* dan sebagai titik integrasi sistem (Tanjung and Haerudin, 2022). Manajemen AD *On-premise* dan terpusat menjadi pilihan selama ini, namun di samping kesederhanaan konsep AD saat ini ternyata terdapat beberapa potensi bahaya.

Pertama, penyalahgunaan akses karena tiap entitas hanya dipisahkan pada *level* OU (*Organitation Unit*), yang artinya secara tidak langsung antar entitas bisa saling komunikasi karena berada di atau *Forest Domain* yang sama. Kedua, semua Bisnis Unit mengikuti setiap kebijakan (*policy*) *Domain* yang notabene tidak selalu sesuai dengan kebutuhan seluruh BU, sehingga fleksibilitas tiap Bisnis Unit dalam mengelola *user* maupun *computer* miliknya terbatasi. Ketiga, saat ini setiap *user* memiliki tiga akun berbeda (*login* komputer, *email* dan jaringan) dan terakhir dampak terbesarnya adalah jika *server* AD *On-premise* tersebut bermasalah, maka semua BU tersebut akan terdampak dan *Corporate* IT akan bertanggung jawab penuh atas risiko tersebut. Oleh karena itu, pihak *Corporate* merasa sudah saatnya tiap BU mulai mengelola secara mandiri. Dengan memanfaatkan salah satu fitur *Office365* yaitu *Microsoft* EntraID nantinya tiap BU akan memiliki AD *On-premise* yang terhubung ke masing-masing EntraID dan dimanfaatkan untuk *Single Sign-On login* komputer, *email* dan jaringan. Saat ini EntraID menjadi penting karena perannya dalam memfasilitasi identitas manajemen layanan berbasis *cloud* (Haimed, Albahar and Alzubaidi, 2023).

Berdasarkan beberapa penelitian yang telah dilakukan sebelumnya diketahui SMP Bani Taqwa Bekasi berhasil membangun *File Server* yang terintegrasi dengan AD (Tanjung and Haerudin, 2022). Selanjutnya pemanfaatan AD sebagai fungsi manajemen akses kontrol pada PT Flextronics Technology Indonesia (Haeruddin and Pangaribuan, 2021). Di tahun sebelumnya manajemen pengguna dan grup AD pun berhasil diintegrasikan dengan sebuah teknologi .NET (Devi Kunia, 2019), lalu di tahun yang sama PT Kudo Teknologi Indonesia mengimplementasikan RADIUS *server* dengan *user* AD *On-premise* untuk proses otentikasinya (Pratama, 2019).

Penelitian ini mengambil studi kasus pada PT X yang berlokasi di Jakarta Pusat yang memiliki permasalahan utama pada manajemen *user* dan *computer* dalam skala besar, di mana saat ini tiap BU masih bergantung penuh pada *Corporate* IT pusat, belum memiliki kendali penuh terhadap *resource* masing-masing dan koneksi antar BU masih bersifat *Trusted Connection*.




Gambar 1. Skema AD Saat Ini

Berdasarkan gambar di atas diketahui bahwa terdapat dua *server* ADDS *On-premise* yang berjalan saat ini, DC (*Domain Controller*) pertama berfungsi sebagai manajemen *user* dan *computer*, DC kedua khusus untuk otentikasi jaringan dengan protokol RADIUS (*Remote Authentication Dial-In User Service*). RADIUS merupakan suatu mekanisme akses kontrol yang mengecek *user* berdasarkan pada mekanisme otentikasi berupa metode *challenge/response* (Pratama, 2019). Kemudian untuk kebutuhan *email*, pengguna mengakses langsung via *internet* dengan akun masing-masing ke portal

*Microsoft Office365*. Dengan kondisi tersebut artinya tiap *user* memiliki tiga akun yang berbeda yakni untuk *login* komputer, jaringan dan *email*.

## 2. METODE

Metode penelitian yang digunakan adalah metode penelitian kualitatif, metode ini digunakan untuk meneliti pada tempat yang alamiah dan dalam pengumpulan datanya berdasarkan pandangan dari sumber data, bukan pandangan peneliti. Jenis data kualitatif tidak bisa diperoleh secara langsung, melainkan melalui suatu proses dengan teknik analisis mendalam pada sebuah objek penelitian (Mustofa and Ramayanti, 2020).

Sedangkan dalam pengembangannya menggunakan metode PPDIOO (*Prepare, Plan, Design, Implement, Operate, dan Optimize*) yaitu metode perancangan jaringan dari Cisco sebagai suatu siklus hidup layanan jaringan dalam mendukung pengembangan jaringan komputer (Setiyani, 2019).


Gambar 2. Metode PPDIOO

*a. Prepare*

Pada tahap ini dilakukan persiapan yang meliputi studi pustaka, wawancara, observasi terhadap objek penelitian serta melakukan pengamatan struktur AD serta jumlah entitas beserta jumlah *user* dan *computer* saat ini.

*b. Plan*

Tahap ini merupakan tahap perencanaan yang meliputi penjadwalan perancangan, pengujian, serta optimalisasi sistem.

*c. Design*

Tahap ini merupakan tahap perancangan sistem dengan menentukan skema AD yang paling sesuai dengan lingkungan IT PT X.

*d. Implementation*

Pada tahap ini dilakukan instalasi *server* ADDS *On-premise* dengan OS *Windows Server* 2022, pengaturan koneksi antara AD *On-premise* dengan EntraID, pembuatan *user* AD dan kemudian melakukan proses sinkronisasi dari AD *On-premise* ke EntraID.

*e. Operate*

Tahap ini merupakan tahap operasional dimana skema usulan diuji dengan memastikan apakah *user* AD yang dibuat sebelumnya dapat digunakan dengan baik pada komputer *client*.

*f. Optimize*

Sistem akan dioptimalisasikan dengan cara memanfaatkaan *user* yang digunakan untuk *login* komputer dan *email* sebagai autentiksi RADIUS jaringan lokal.

Penelitian ini berlangsung selama 2 (dua) bulan pada kantor pusat PT X yang beralamatkan di Cempaka Putih, Jakarta Pusat, DKI Jakarta. Dalam penelitian ini, penulis melakukan studi literatur, observasi, dan wawancara langsung dan semi terstruktur kepada beberapa *stakeholder* terkait, termasuk Manajer *Hybrid Cloud* dan Kepala Manajer *Infrastructure IT* PT X untuk mengetahui kendala yang tengah dihadapi dan menilai gambaran ekspektasi kondisi kedepannya. Layaknya wawancara terstruktur, wawancara jenis ini juga menguraikan topik dan pertanyaan yang disiapkan oleh peneliti, namun dalam prosesnya tidak ada kepatuhan yang kaku (Yuliansyah and Soewito, 2020).

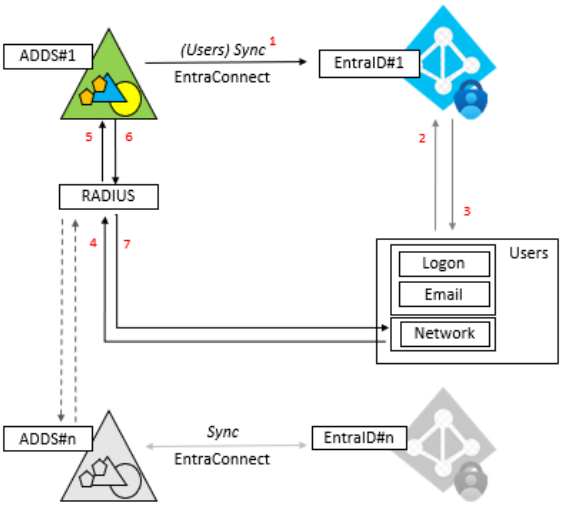
## 3. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk merancang sebuah skema AD yang sesuai dengan kebutuhan dan IT *environment* PT X saat ini. Skema AD usulan mengacu pada beberapa aspek tujuan seperti efisien secara biaya, sederhana dalam operasional, fleksibel dalam pengelolaan, dan agile terhadap kemajuan teknologi di masa mendatang.

### 3.1. Skema AD Usulan

Pada perancangan skema AD usulan, ketiga akun otentikasi (*login*, jaringan dan *email*) yang sebelumnya terpisah tersebut kedepannya akan dibuat SSO (*Single Sign-On*) dengan memanfaatkan sebuah akun EntraID yang secara data tersinkronisasi satu arah dari

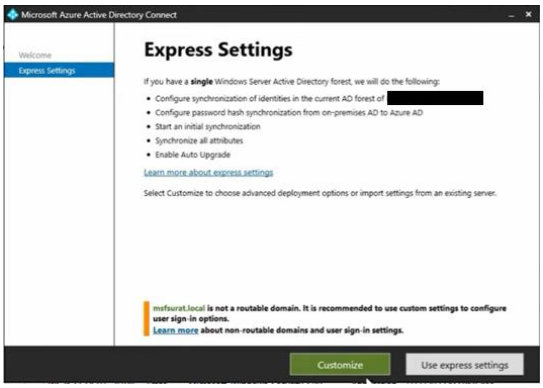
sebuah ADDS *On-premise* yang nantinya digunakan juga untuk otentikasi jaringan lokal menggunakan protokol RADIUS.




Gambar 3. Skema AD Usulan

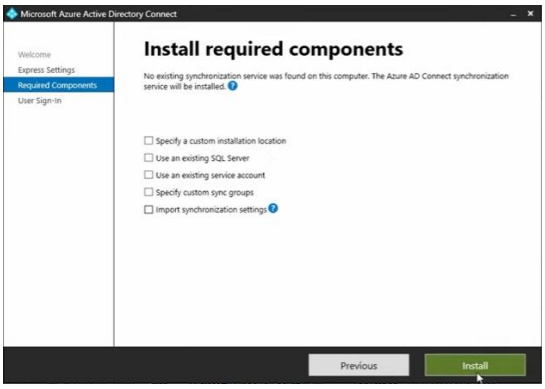
### 3.2. Konfigurasi Koneksi AD *On-premise* dan EntraID

Sebelumnya kita perlu membangun koneksi antara AD *On-premise* dengan EntraID dengan cara menginstal *Microsoft* Entra Connect (sebelumnya dikenal sebagai Azure AD Connect), sebuah aplikasi *Microsoft* yang mengintegrasikan AD *On-premise* dan EntraID dengan lancar, khususnya memberi akses *user* melakukan SSO. Setelah kita *download* dan *install* Entra *Connect* langkah pertama kita pilih *Customize Settings*.



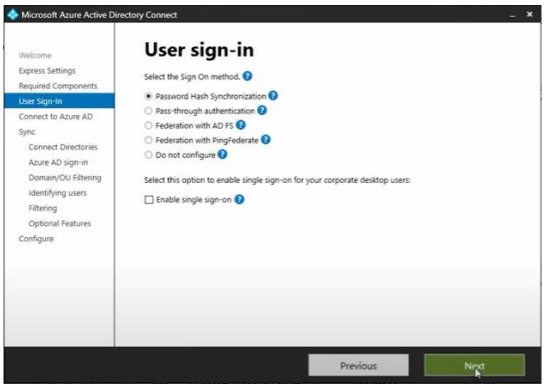

Gambar 4. Tampilan Awal EntraID *Connect*

Langkah selanjutnya dikarenakan konsep ini merupakan implementasi awal kita cukup *skip* proses *Required Components*, klik *Install*.



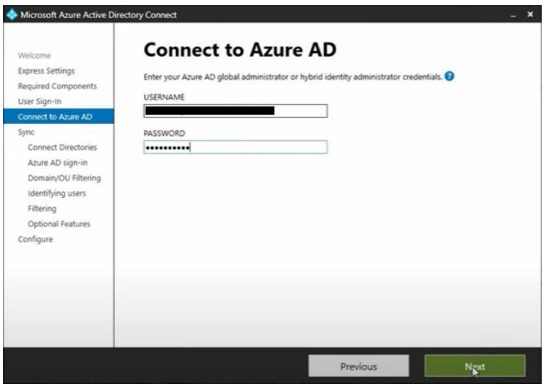

Gambar 5. *Required Components*

Kemudian pilih PHS (Password Hash Synchronization) sebagai metode *User Sign-in* yang sering digunakan untuk penerapan *hybrid indentity* dalam melakukan sinkronisasi *password user* dari *On-premise* AD ke EntraID. Dengan metode PHS otentikasi *user* secara *default* akan ditangani oleh EntraID, sementara proses operasional sepenuhnya berada di AD *On-premise*.




Gambar 6. Metode *User Sign-in*

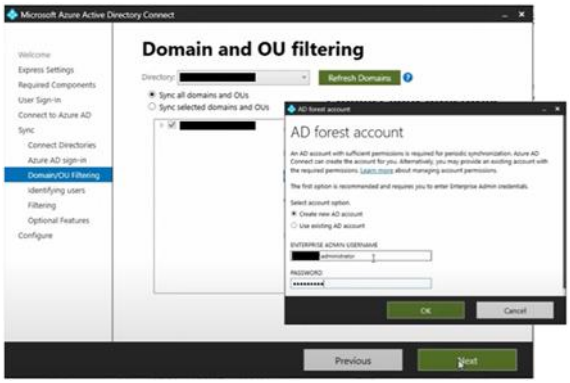
Selanjutnya masukan akun EntraID yang memiliki akses level *Global Administrator* sebagai syarat otentikasi koneksi antara AD *On-premise* dengan EntraID.




Gambar 7. *Global Administrator Credential*

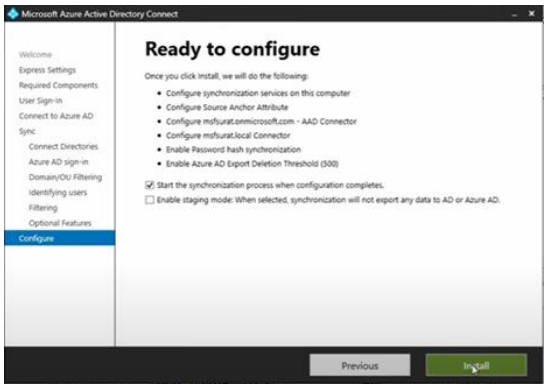
Kemudian tentukan *Domain* maupun OU(*Organization Unit*) pada AD *On-premise*

yang akan disinkronisasi dengan EntraID, di mana proses tersebut membutuhkan otentikasi berupa *user* AD *On-premise* dengan level akses *Domain Admins*.




Gambar 8. Pemilihan *Domain* dan OU

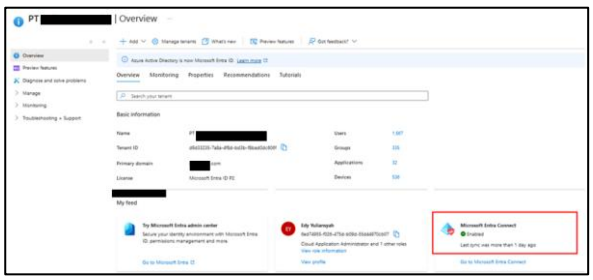
Pastikan kembali konfigurasi sudah sesuai, terakhir pilih *Install* untuk memulai proses sinkronisasi antara AD *On-premise* dengan EntraID.




Gambar 9. Konfirmasi Konfigurasi

### 3.2.1 **Pengecekan Koneksi Antara AD *On-premise* Dengan EntraID**

Untuk memastikan bahwa koneksi AD dan EntraID sudah terbangun dapat dilihat pada tampilan *Overview* dalam *Dashboard* EntraID, kemudian pada bagian *Microsoft* Entra *Connect* akan berstatus *Enabled*.



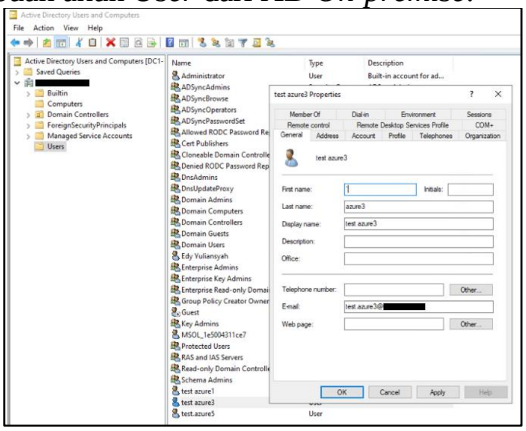
Gambar 10. Status *Microsoft* EntraConnect

## 3.3. **Pembahasan**

Tahap ini merupaka tahap melakukan uji coba dan hasil dari sistem jaringan yang diterapkan pada objek penelitian.

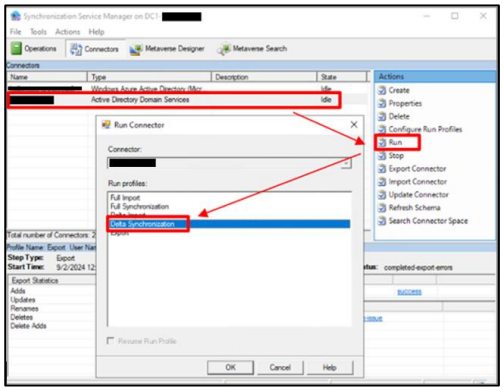
### 3.3.1 **Uji Coba Sinkronisasi AD *On-premise* ke EntraID**

Uji coba ini bertujuan untuk membuktikan antara AD *On-premise* dan EntraID sudah dapat berkomunikasi dengan cara membuat sebuah akun *User* dari AD *On-premise*.



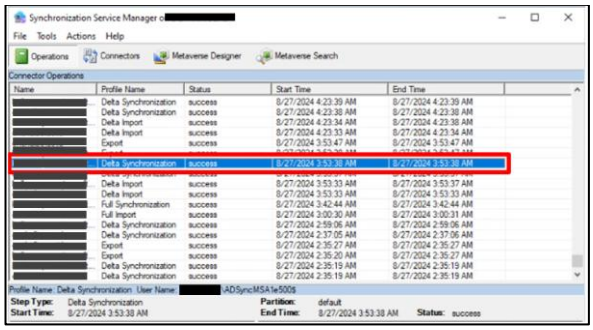
Gambar 11. Pembuatan Akun *User*

Kemudian, kita lakukan sinkronisasi secara *manual* dengan membuka *Synchronization Service Manager* yang terdapat pada *server* AD *On-premise* yang telah terinstal bersamaan dengan EntraID *Connect*, pilih ADDS atau *Domain*, klik *Run*, kemudian pilih *Delta Synchronization*.



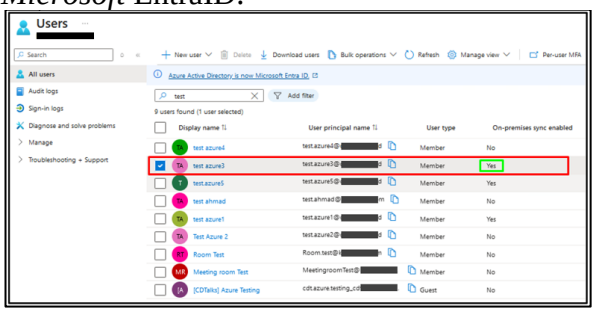

Gambar 11. Sinkronisasi *Manual User* AD

Tunggu beberapa saat dan pastikan proses sinkronisasi selesai dan berstatus *success*.



Gambar 12. Status Sinkronisasi AD

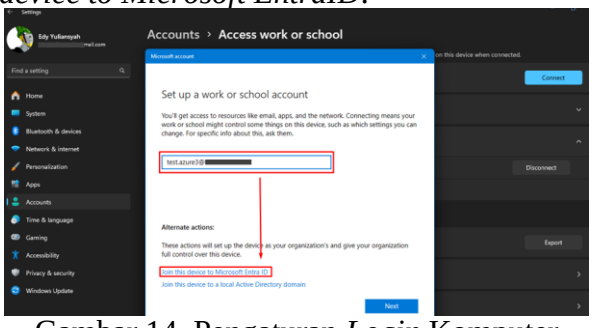
Kemudian masuk ke *Dashboard All User* pada *Microsoft* EntraID, kemudian cari *Username* yang sebelumnya dibuat melalui AD *On-premise*. Jika berhasil maka *user* tersebut akan muncul dengan status *On-premise sync enabled=Yes*, artinya *user* tersebut berasal dari AD *On-premise* dan berhasil tersinkron ke dalam direktori *Users Microsoft* EntraID.



Gambar 13. *List* Akun EntraID

### 3.3.2 **Uji Coba *Join Device* Melalui EntraID**

Uji coba ini bertujuan untuk membuktikan *user* yang telah dibuat melalui AD *On-premise* dan tersinkronisasi ke direktori EntraID dapat digunakan untuk *login* Windows di komputer *client*. Masuk ke menu *Settings*, pilih *Set up work or school account*, masukkan *user* yang sebelumnya kita buat, kemudian pilih *Join this device to Microsoft EntraID*.

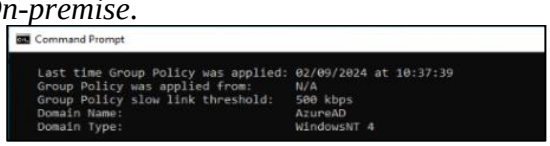


Gambar 14. Pengaturan *Login* Komputer

Setelah test.azure3 berhasil ditambahkan, selanjutnya kita coba *login* Windows dengan *user* tersebut. Kemudian kita masuk *command prompt* lalu ketik *gpresult* /R untuk memastikan *Domain Name* yang terhubung. Di sini dapat kita lihat bahwa yang terpasang adalah *Domain Name* dari *server* AD *On-premise*, kondisi tersebut karena *user* test.azure3 merupakan *user* yang dibuat dari AD *On-premise* yang kemudian akan tersinkronisasi ke EntraID.

Gambar 15. *On-premise Domain Name*

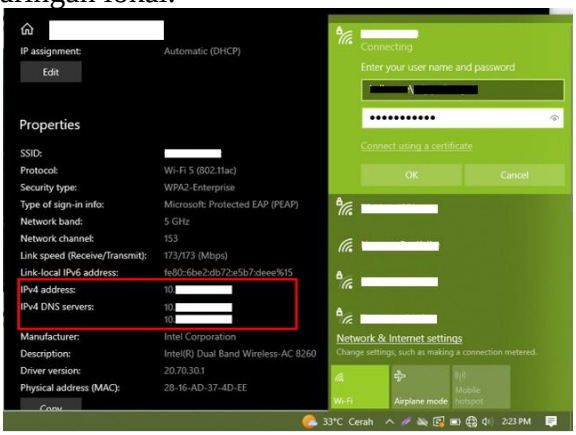
Sementara ketika menggunakan *user* yang dibuat langsung dari EntraID, *Domain Name* yang terpasang adalah AzureAD, artinya *user* tersebut memang dibuat melalui EntraID sehingga tidak memiliki korelasi dengan AD *On-premise*.



Gambar 16. EntraID *Domain Name*

### 3.3.3 **Optimalisasi Otentikasi Jaringan**

Setelah akun *user* dapat digunakan di komputer *client*, selanjutnya kita manfaatkan *user* tersebut untuk otentikasi RADIUS pada jaringan lokal. Cari nama SSID jaringan lokal tujuan kemudian pilih *Connect*, kemudian masukkan *username* dan *password* akun test.azure3. Untuk mengetahui keberhasilan proses otentikasi, pada *Properties* SSID pastikan kita telah mendapatkan IPv4 *Address* jaringan lokal.



Gambar 17. Otentikasi RADIUS

## 4. PENUTUP

### 4.1. Kesimpulan

Konsep *Hybrid Active Directory* berhasil terbangun pada *IT environment* PT X dengan skema sinkronisasi *User* satu arah dari AD *On-premise* ke EntraID. Konsep ini memanfaatkan

akun EntraID sebagai akun tunggal untuk fungsi otentikasi *login*, *email* serta jaringan. Konsep ini lebih efektif dibandingkan dengan konsep AD saat ini yang masih menggunakan tiga akun berbeda untuk tiap otentikasinya. Kekurangan penelitian ini adalah sinkronisasi yang hanya dapat satu arah, fitur *password writeback* belum memungkinkan diterapkan saat ini karena ada biaya *license* tambahan khusus fitur tersebut dan secara operasional utamanya masih berada di AD *On-premise*.

### 4.2. Saran

Untuk penelitian selanjutnya dapat dicoba memanfaatkan fitur yang tersedia di beberapa model *license* lainnya, termasuk *password writeback* supaya tiap *user* dapat melakukan *self-service* terhadap akunnya masing-masing saat berada di jaringan luar kantor. Membuat sebuah *web portal* atau dapat memanfaatkan *third-party applications* yang memungkinkan manajemen seluruh AD secara terpusat.

## 5. DAFTAR PUSTAKA

Devi Kunia, P. (2019) 'Implementasi Aplikasi Manajemen Pengguna Dan Grup Berbasis Active Directory Menggunakan Teknologi .Net', Jurnal Manajemen Informatika, 6(1), pp. 7–15.

Haeruddin, H. and Pangaribuan, B.F. (2021) 'Perancangan Dan Implementasi Active Directory Domain Controller Menggunakan Windows Server 2012 R2 Di Pt. Flextronics Technology Indonesia', National Conference for Community Service Project (NaCosPro), 3(1), pp. 1150–1154. Available at: https://ojs.digitalartisan.co.id/index.php/nacospro/article/view/6067.

Haimed, I.B., Albahar, M. and Alzubaidi, A. (2023) 'Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks', Future Internet, 15(7), pp. 1–18. Available at: https://doi.org/10.3390/fi15070226.

Mustofa, A. and Ramayanti, D. (2020) 'Implementasi Load Balancing dan Failover to Device Mikrotik Router Menggunakan Metode NTH (Studi Kasus: PT.GO-JEK Indonesia)', Jurnal Teknologi Informasi dan Ilmu Komputer, 7(1), p. 139. Available at: https://doi.org/10.25126/jtiik.2020701638.

Pratama, R.W. (2019) 'Implementasi Sistem Otentikasi User Menggunakan Radius Server Dan Active Directory Pada Jaringan Wireless Di PT . Kudo Teknologi Indonesia', ResearchGate [Preprint], (April 2019).

Setiyani, L. (2019) 'Peningkatan Layanan Jaringan Internet Menggunakan Teknik Load Balancing pada Balai Besar Pelatihan Kesehatan Ciloto', Faktor Exacta, 12(2), p. 112. Available at: https://doi.org/10.30998/faktorexacta.v12i2.3668.

Tanjung, D. and Haerudin, H. (2022) 'Implementasi File Server Terintegrasi dengan Active Directory pada SMP Bani Taqwa Kota Bekasi', OKTAL : Jurnal Ilmu Komputer dan Science , 1(7), pp. 986–996. Available at: https://journal.mediapublikasi.id/index.php/oktal/article/view/405.

YULIANSYAH, E. and SOEWITO, B. (2020) 'Asynchronous multi-site method design disaster recovery center on the business process automotive manufacturing (case study: Pt xyz)', Journal of Theoretical and Applied Information Technology, 98(15), pp. 3060–3079.