PT Jurnal Cendekia Indonesia
Journal of Information Systems and Business Technology
Homepage: https://journal.jci.co.id/jisbt
Vol. 02 No. 04 (2026) Page: 150-155
E-ISSN: 3109-8886

Perancangan Active Directory untuk Pengelolaan IT SMA Muhammadiyah 1 Tangerang dengan Metode PPDIOO

Bobby Hertantyo[1], Salman Farizy[2]

[12]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia

[*]Corresponding Author Email: bobbyhrt1@gmail.com

Abstract

Prior to this study, the computer laboratory at SMA Muhammadiyah 1 Tangerang operated under a workgroup scheme in which each machine kept its own user accounts, device settings, and security rules independently. This setup slowed administrative work, left configurations inconsistent, and made centralized oversight difficult to achieve. To address this, the present study builds a centralized Active Directory Domain Services (AD DS) environment on Windows Server 2022 for managing users and network policy, following the six-stage PPDIOO framework (Prepare, Plan, Design, Implement, Operate, Optimize). The build-out includes setting up a Domain Controller with DNS and DHCP services, structuring Organizational Units (OU) and Security Groups, defining Group Policy Objects (GPO), and applying Role-Based Access Control (RBAC). Functional verification relied on Black Box Testing across authentication, network connectivity, name resolution, IP assignment, domain-join, password policy, and GPO-restriction scenarios. Across all seventeen test scenarios, the outcomes were valid: client machines joined the domain without issue, authentication behaved as designed, DNS and DHCP responded correctly, and GPO restrictions were applied consistently with each user's role. Overall, the AD DS deployment raised administrative efficiency, kept configurations consistent, and strengthened security across the school's IT resources.

Keywords: *Active Directory Domain Services, Windows Server 2022, Group Policy Object, Role-Based Access Control, PPDIOO.*

Abstrak

Sebelum penelitian ini dilakukan, laboratorium komputer SMA Muhammadiyah 1 Tangerang dikelola dengan pola workgroup, di mana setiap komputer menyimpan akun pengguna, konfigurasi perangkat, dan kebijakan keamanannya sendiri-sendiri. Pola kerja seperti ini membuat proses administrasi berjalan lambat, konfigurasi antarkomputer tidak seragam, dan pengawasan terpusat sulit diwujudkan. Untuk mengatasi hal tersebut, penelitian ini membangun lingkungan Active Directory Domain Services (AD DS) berbasis Windows Server 2022 yang terpusat guna mengelola pengguna dan kebijakan jaringan, dengan mengikuti kerangka kerja PPDIOO yang terdiri atas enam tahap (Prepare, Plan, Design, Implement, Operate, Optimize). Pembangunan sistem ini mencakup penyiapan Domain Controller beserta layanan DNS dan DHCP, penyusunan Organizational Unit (OU) dan Security Group, penetapan Group Policy Object (GPO), serta penerapan Role-Based Access Control (RBAC). Verifikasi fungsi sistem dilakukan melalui Black Box Testing terhadap skenario autentikasi, konektivitas jaringan, resolusi nama, pemberian alamat IP, join domain, kebijakan password, dan pembatasan melalui GPO. Dari tujuh belas skenario pengujian, seluruhnya dinyatakan valid: komputer client bergabung ke domain tanpa kendala, autentikasi domain berjalan sesuai rancangan, DNS maupun DHCP merespons dengan benar, dan pembatasan GPO diterapkan konsisten sesuai peran pengguna. Secara keseluruhan, penerapan AD DS ini berhasil mendongkrak efisiensi administrasi, menjaga konsistensi konfigurasi, dan memperkuat keamanan pengelolaan sumber daya IT sekolah.

Kata Kunci: Active Directory Domain Services, Windows Server 2022, Group Policy Object, Role-Based Access Control, PPDIOO.

A. PENDAHULUAN

Di lingkungan sekolah, laboratorium komputer menjadi salah satu sarana penting yang menopang proses belajar berbasis teknologi, baik untuk kegiatan praktikum maupun untuk melatih kemampuan siswa dalam menggunakan komputer dan jaringan. Supaya kegiatan tersebut dapat berjalan lancar, infrastruktur teknologi informasinya perlu dikelola dengan baik agar sistem tetap aman, administrasi tidak merepotkan, dan layanan tetap tersedia bagi semua penggunanya.

Hasil pengamatan di Laboratorium Komputer SMA Muhammadiyah 1 Tangerang menunjukkan bahwa pengelolaan komputer di sana masih memakai pola workgroup, artinya setiap unit memiliki akun lokal dan

Diterima Redaksi: 15-08-2026 | Selesai Revisi: 19-08-2026 | Diterbitkan Online: 20-08-2026

konfigurasinya sendiri sehingga administrator terpaksa mengatur satu per satu perangkat secara terpisah. Pembuatan akun baru, penggantian kata sandi, dan perubahan konfigurasi masih dilakukan secara manual, akibatnya proses administrasi memakan waktu lebih panjang, apalagi bila ada kebijakan baru yang mesti diberlakukan ke seluruh komputer sekaligus. Selain merepotkan, pola ini juga membawa risiko keamanan sebab satu akun pengguna tidak bisa dipakai di semua komputer, hak akses belum diatur berdasarkan peran, dan belum ada cara untuk menerapkan kebijakan keamanan secara terpusat maupun merekam aktivitas pengguna.

Guna mengatasi permasalahan tersebut, penelitian ini membangun Active Directory Domain Services (AD DS) di atas Windows Server 2022 sebagai pusat pengelolaan akun pengguna, komputer, serta sumber daya jaringan, sebagaimana direktori terpusat semacam ini terbukti meningkatkan pengendalian akses dan keamanan data pada berbagai instansi (Jumarta et al., 2025; Taberima & Ramayanti, 2024). Dengan adanya Domain Controller, administrator bisa mengurus akun, hak akses, dan proses autentikasi dari satu titik kendali saja, sedangkan Group Policy Object (GPO) memungkinkan berbagai aturan keamanan diberlakukan secara otomatis ke seluruh komputer yang tergabung dalam domain, yang efektivitasnya dalam menegakkan kebijakan keamanan secara konsisten turut didukung oleh (Budiyanto & Herawatie, 2023; Muhamad et al., 2025). Tahapan implementasinya mengacu pada metode PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) karena metode ini memberikan alur kerja yang runtut, mulai dari mengenali kebutuhan, menyusun rancangan, menjalankan implementasi, mengoperasikan sistem, hingga mengevaluasi hasilnya, sebagaimana kerangka kerja ini juga terbukti efektif dalam sejumlah perancangan jaringan sekolah (Ajrina et al., 2024; Putri Arini et al., 2021).

Mengacu pada uraian di atas, penelitian ini berupaya menjawab tiga pertanyaan: (1) seperti apa kondisi pengelolaan pengguna dan kebijakan jaringan sebelum Active Directory diterapkan; (2) bagaimana tahapan penerapan Active Directory Domain Services dalam mengelola akun pengguna, grup, dan kebijakan jaringan; dan (3) sejauh mana penerapan Active Directory memengaruhi efektivitas pengelolaan pengguna serta keamanan sumber daya IT. Adapun tujuan penelitian ini adalah mengkaji kondisi sistem yang sedang berjalan, merancang serta menerapkan AD DS beserta GPO sebagai solusi pengelolaan pengguna dan keamanan jaringan, dan menilai efektivitasnya lewat pengujian sistem.

B. METODE

Data penelitian dikumpulkan lewat beberapa cara, yaitu pengamatan langsung atas kondisi jaringan dan pengelolaan pengguna di laboratorium, wawancara bersama administrator untuk menggali kendala dan kebutuhan sistem, kajian pustaka atas jurnal dan referensi seputar Active Directory maupun metode PPDIOO, serta pendokumentasian struktur jaringan dan konfigurasi yang sedang berjalan.

Perangkat yang dipakai dalam implementasi terdiri dari satu unit komputer server yang berperan sebagai Domain Controller (setara Intel Core i5 Generasi 8, RAM 16 GB, SSD NVMe 1TB, menjalankan Windows Server 2022) dan beberapa komputer client (setara Intel Core i5 Gen8, RAM 8 GB, Windows 10 Enterprise), yang semuanya tersambung dalam jaringan LAN bertopologi star melalui switch gigabit. Selama proses implementasi dan pengujian, virtualisasi dijalankan menggunakan Microsoft Hyper-V. Pengalamatan IP mengikuti subnet privat kelas C 192.168.1.0/24, dengan Domain Controller menempati IP statis 192.168.1.10, sedangkan komputer client memperoleh IP dinamis pada rentang 192.168.1.50–254 melalui DHCP Server.

Sistem dikembangkan mengikuti enam tahap dalam metode PPDIOO. Pada tahap Prepare, kebutuhan awal dan persoalan pengelolaan jaringan sekolah diidentifikasi. Tahap Plan digunakan untuk menyusun kebutuhan perangkat keras, perangkat lunak, dan kebijakan keamanan yang hendak diberlakukan. Tahap Design mencakup perancangan arsitektur Active Directory, meliputi struktur domain, Organizational Unit (OU), pembagian grup pengguna berdasarkan peran (RBAC), dan kebijakan GPO. Pada tahap Implement, konfigurasi Domain Controller, DNS, DHCP, OU, akun pengguna, grup, serta GPO diterapkan menggunakan Windows Server 2022. Tahap Operate memastikan sistem berjalan sebagaimana mestinya melalui proses login pengguna, pemberlakuan kebijakan, dan pemantauan aktivitas. Terakhir, tahap Optimize dipakai untuk mengevaluasi dan menyempurnakan sistem berdasarkan hasil pengujian yang diperoleh.

Untuk mengevaluasi sistem, digunakan metode Black Box Testing yang menguji fungsionalitas berdasarkan masukan dan keluaran sistem tanpa perlu menelusuri struktur kode di dalamnya. Cakupan pengujiannya meliputi autentikasi login, konektivitas jaringan, resolusi nama melalui DNS, pembagian alamat IP oleh DHCP, proses join domain, kebijakan kata sandi, serta keefektifan pembatasan akses melalui GPO.

C. HASIL DAN PEMBAHASAN

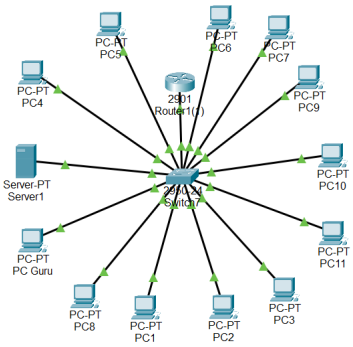
Bagian ini membahas hasil perancangan topologi jaringan, penerapan layanan inti Active Directory (Domain Controller, DNS, dan DHCP), penyusunan struktur direktori berbasis peran, penerapan Group Policy Object, serta hasil pengujian sistem yang dilakukan lewat metode Black Box Testing.

Perancangan Topologi Jaringan

Jaringan dirancang dengan topologi star, di mana seluruh komputer client dihubungkan ke satu switch pusat yang kemudian tersambung ke Domain Controller, seperti terlihat pada Gambar 1. Pilihan topologi ini didasarkan pada kemudahan administrasi, fleksibilitasnya bila ada penambahan perangkat, serta kemampuannya mengisolasi gangguan pada satu perangkat tanpa mengganggu perangkat lain di jaringan yang sama. Dalam skema pengalamatan IP, Domain Controller menempati alamat statis 192.168.1.10 sekaligus berperan sebagai server utama DNS dan AD DS, router/gateway berada di

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

192.168.1.1, sementara seluruh komputer laboratorium mendapat alamat dinamis pada rentang 192.168.1.50 sampai 192.168.1.254 melalui DHCP Server.

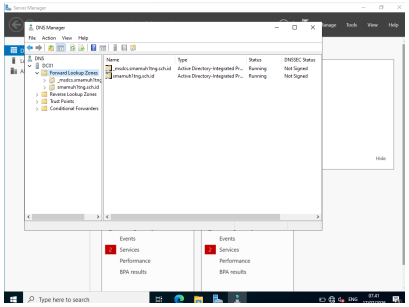


Gambar 1. Topologi Jaringan yang Diusulkan

Implementasi Domain Controller, DNS Server, dan DHCP Server

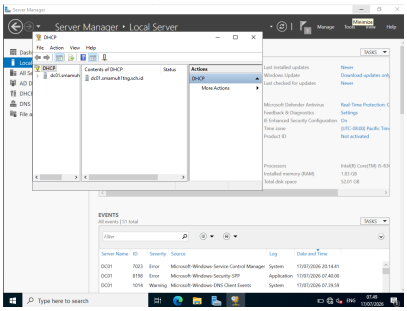
Tahap implementasi dimulai dengan memasang Windows Server 2022 pada lingkungan virtual Hyper-V, kemudian server tersebut dipromosikan menjadi Domain Controller dengan menambahkan role Active Directory Domain Services (AD DS) sekaligus membentuk domain baru bernama smamuh1tng.sch.id. Begitu proses promosi rampung dan server melakukan restart, Domain Controller pun berfungsi sebagai pusat autentikasi dan direktori bagi seluruh objek pengguna, komputer, dan kebijakan di jaringan laboratorium.

Konfigurasi layanan DNS Server dilakukan bersamaan dengan promosi Domain Controller, mencakup forward lookup zone maupun reverse lookup zone, sehingga komputer client mampu menerjemahkan nama domain (hostname) menjadi alamat IP yang sesuai sekaligus menemukan letak Domain Controller di jaringan; keandalan layanan DNS semacam ini berpengaruh besar terhadap kelancaran resolusi nama pada jaringan yang menuntut ketersediaan tinggi (Pratama et al., 2024). Tampilan antarmuka DNS Manager pada Windows Server 2022 setelah zona domain berhasil dikonfigurasi dapat dilihat pada Gambar 2.



Gambar 2. Antarmuka DNS Manager pada Windows Server 2022

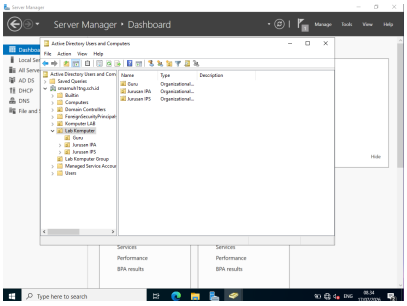
Setelah itu, role DHCP Server dipasang dan dikonfigurasi agar mampu membagikan alamat IP secara otomatis ke komputer client sesuai scope 192.168.1.50–254, lengkap dengan pengaturan default gateway, DNS Server, dan lease duration. Berkat konfigurasi ini, administrator tak lagi harus mengatur IP address satu per satu pada setiap komputer client, sebab alamat IP, subnet mask, gateway, dan DNS Server sudah diberikan secara otomatis begitu komputer terhubung ke jaringan. Konsol manajemen DHCP setelah scope-nya diaktifkan ditampilkan pada Gambar 3.



Gambar 3. Antarmuka Konsol Manajemen DHCP Server

Perancangan Struktur Direktori dan Role-Based Access Control (RBAC)

Struktur direktori disusun secara berjenjang melalui Organizational Unit (OU) untuk mengelompokkan objek pengguna dan komputer berdasarkan peran masing-masing di organisasi sekolah. Diawali dengan pembentukan OU induk “Lab Komputer”, yang kemudian dipecah lagi menjadi beberapa sub-OU, yakni “Guru”, “Jurusan IPA”, dan “Jurusan IPS”, seperti ditampilkan pada Gambar 4. Struktur berjenjang seperti ini mempermudah penerapan kebijakan yang berbeda-beda antarkelompok pengguna tanpa mengganggu kelompok lainnya.



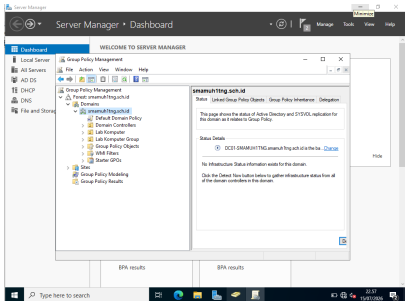
Gambar 4. Struktur Sub-Organizational Unit pada Active Directory

Di setiap OU dibuat Security Group, misalnya grup untuk seluruh pengguna (ALL Users) maupun grup berdasarkan peran, yang keanggotaannya diatur dengan mencari objek pengguna di Active Directory Users and Computers. Perpaduan antara OU dan Security Group inilah yang menjadi dasar penerapan Role-Based Access Control (RBAC): hak akses dan kebijakan keamanan tidak perlu diberikan satu per satu ke setiap pengguna, melainkan otomatis mengikuti keanggotaan grup dan posisi OU pengguna dalam struktur direktori. Cara ini membuat proses administrasi jadi lebih sederhana, karena menambahkan pengguna baru cukup dilakukan dengan memasukkannya ke OU dan grup yang tepat, sejalan dengan (Moch Afdal Dzikri Maulana, Arip Solehudin, 2026) yang menunjukkan bahwa penerapan RBAC pada Active Directory Domain Service mempermudah pengaturan hak akses sekaligus meminimalkan risiko pemberian izin yang berlebihan.

Implementasi Group Policy Object (GPO)

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Pengelolaan Group Policy Object dilakukan lewat konsol Group Policy Management (GPMC), yang menampilkan struktur domain beserta OU tempat masing-masing kebijakan diterapkan, sebagaimana terlihat pada Gambar 5. Setiap OU memiliki GPO tersendiri; misalnya, kebijakan untuk OU Siswa mencakup Prevent Access to Control Panel and PC Settings, Prohibit Access to Command Prompt, Prevent Access to registry editing tools, serta pembatasan penggunaan Removable Disks guna mencegah penyalinan data lewat media penyimpanan eksternal. Selain itu, diberlakukan pula kebijakan pembatasan aplikasi sehingga hanya program tertentu, seperti perangkat lunak perkantoran, yang boleh dijalankan oleh siswa maupun guru pada komputer laboratorium, sebagaimana pembatasan semacam ini terbukti efektif memitigasi risiko keamanan server (Muhamad et al., 2025).



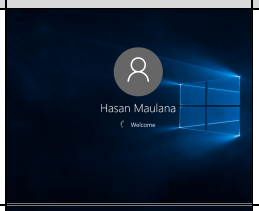
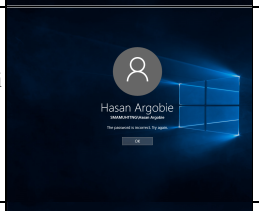
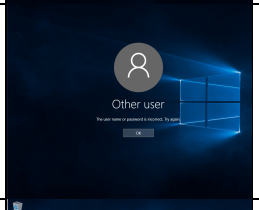
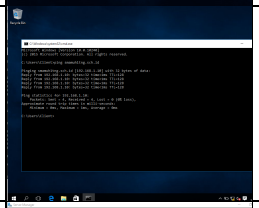
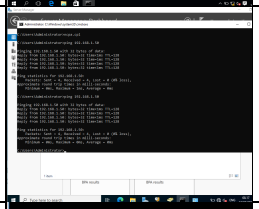
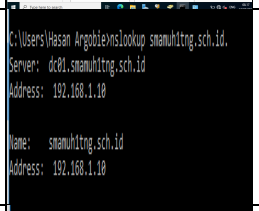
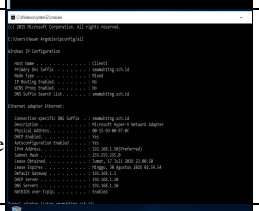
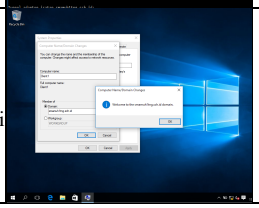
Gambar 5. Struktur Domain dan Organizational Unit pada Konsol Group Policy Management

Setiap GPO yang sudah dikonfigurasi kemudian ditautkan (link) ke OU yang bersangkutan, dan status penautannya diverifikasi melalui GPMC. Lewat mekanisme ini, kebijakan keamanan berlaku otomatis untuk seluruh komputer maupun akun pengguna di OU tersebut tanpa harus dikonfigurasi ulang satu per satu, dan kebijakan itu akan tetap berlaku pula ketika ada penambahan pengguna atau komputer baru ke OU yang sama.

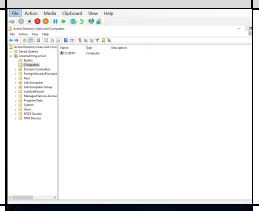
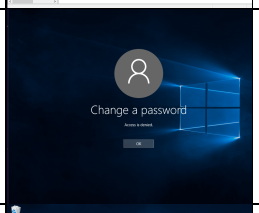
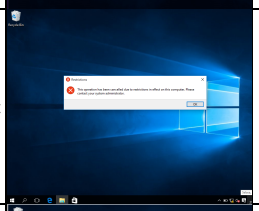
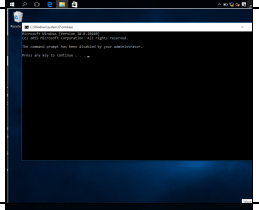
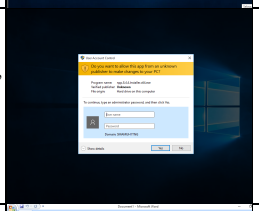
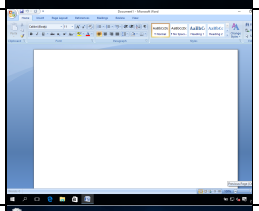
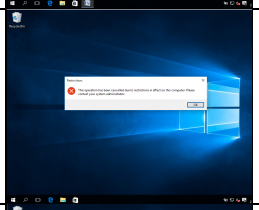
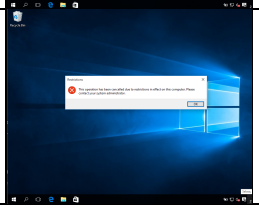
Pengujian Sistem

Sistem yang sudah diimplementasikan diuji menggunakan metode Black Box Testing, yakni pengujian yang berfokus pada verifikasi fungsi berdasarkan masukan dan keluaran yang dihasilkan tanpa menelusuri struktur kode maupun proses internal sistem, yang diperlukan untuk memastikan keandalan sistem keamanan sebelum diterapkan pada lingkungan produksi (Harahap & Handoko, 2024). Pengujian ini mencakup tujuh aspek fungsional, yaitu autentikasi login, konektivitas jaringan, resolusi nama DNS, pembagian alamat IP oleh DHCP, proses join domain, kebijakan password, dan efektivitas pembatasan akses lewat Group Policy Object, dengan total tujuh belas skenario uji. Rincian skenario, hasil yang diharapkan, bukti pengujian, serta kesimpulannya disajikan pada Tabel 1.

Tabel 1. Hasil Pengujian Black Box Testing

No	Skenario Uji	Hasil yang Diharapkan	Bukti Pengujian	Simpulan
1	Login dengan akun domain valid	Login berhasil, sistem menampilkan desktop sesuai profil user		Valid
2	Login dengan password salah	Login gagal, muncul notifikasi "The user name or password is incorrect"		Valid
3	Login dengan username tidak terdaftar	Login gagal, sistem menolak akses		Valid
4	Ping dari client ke server	Reply diterima, tidak ada request timed out		Valid
5	Ping dari server ke client	Reply diterima, tidak ada request timed out		Valid
6	Resolusi nama domain (nslookup) dari client	DNS Server mengembalikan IP Address yang sesuai		Valid
7	Resolusi nama Domain Controller (nslookup)	DNS Server mengembalikan IP Address DC01 dengan benar		Valid
8	Client menerima IP otomatis dari DHCP	Client mendapatkan IP Address, Gateway, dan DNS sesuai scope DHCP		Valid
9	Join domain dengan kredensial valid	Muncul pesan "Welcome to the smamuh1tng.sch.id domain"		Valid

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

No	Skenario Uji	Hasil yang Diharapkan	Bukti Pengujian	Simpulan
10	Verifikasi objek komputer di server	Objek komputer client tercatat di Active Directory Users and Computers		Valid
11	User cannot change password	Sistem menolak perubahan password oleh user		Valid
12	Pembatasan akses Control Panel (GPO)	Akses ditolak / menu tidak dapat dibuka		Valid
13	Pembatasan Command Prompt (GPO)	Muncul pesan "The command prompt has been disabled by your administrator"		Valid
14	Pembatasan instalasi aplikasi (GPO)	Instalasi tertahan, membutuhkan kredensial Administrator		Valid
15	Akses aplikasi yang diizinkan (Siswa/Guru)	Aplikasi perkantoran berhasil terbuka dengan normal		Valid
16	Akses aplikasi yang tidak terdaftar (GPO)	Muncul pesan "This operation has been cancelled due to restrictions in effect on this computer"		Valid
17	Pembatasan akses Regedit (GPO)	Akses ditolak, muncul pesan pembatasan pada seluruh utilitas sistem		Valid

Merujuk pada Tabel 1, keseluruhan tujuh belas skenario pengujian dinyatakan valid. Dari sisi autentikasi, sistem dapat membedakan antara akun domain yang sah, password yang keliru, dan username yang tidak terdaftar, sehingga login hanya berhasil bagi pengguna yang memang berhak. Sementara itu, uji konektivitas dan layanan jaringan memperlihatkan bahwa komunikasi antara Domain Controller dan client berjalan mulus, resolusi nama domain lewat DNS bekerja secara akurat, dan pembagian alamat IP melalui DHCP berlangsung otomatis tanpa perlu konfigurasi manual di tiap perangkat.

Dari sisi manajemen keanggotaan domain, komputer client berhasil bergabung ke domain smamuh1tng.sch.id dan langsung tercatat secara otomatis sebagai objek komputer di Active Directory Users and Computers, yang menandakan bahwa mekanisme join domain dan pencatatan objeknya berjalan sesuai rancangan. Adapun dari sisi kebijakan keamanan, sistem berhasil menegakkan aturan password sesuai konfigurasi administrator serta menerapkan pembatasan GPO secara konsisten, contohnya penolakan akses ke Control Panel, Command Prompt, dan Registry Editor, maupun instalasi aplikasi tanpa kredensial Administrator, sementara aplikasi yang memang diizinkan tetap bisa dijalankan secara normal oleh pengguna di OU yang sesuai.

Secara umum, hasil pengujian ini membuktikan bahwa penerapan Active Directory berhasil menggeser pola workgroup ke pengelolaan pengguna dan kebijakan jaringan yang lebih terpusat, konsisten, dan aman. Administrator kini bisa mengurus akun, hak akses, maupun kebijakan keamanan hanya dari satu konsol pusat, berbeda dengan sebelumnya yang mengharuskan setiap perubahan dilakukan satu per satu di tiap komputer. Temuan ini selaras dengan tujuan penelitian, yakni meningkatkan efisiensi administrasi sekaligus keamanan pengelolaan sumber daya IT di laboratorium komputer sekolah.

D. PENUTUP

Simpulan

Penerapan Active Directory Domain Services (AD DS) di atas Windows Server 2022 telah berhasil diwujudkan di Laboratorium Komputer SMA Muhammadiyah 1 Tangerang dengan mengikuti metode PPDIOO sebagai panduan pelaksanaan, mulai dari tahap persiapan sampai optimasi. Layanan Domain Controller, DNS Server, dan DHCP Server berhasil dikonfigurasi dan diintegrasikan sehingga menunjang autentikasi pengguna, pembagian alamat IP secara otomatis, dan komunikasi antarperangkat di dalam domain. Penerapan Organizational Unit, Security Group, dan Role-Based Access Control mengelompokkan pengguna berdasarkan perannya masing-masing sehingga pengelolaan hak akses menjadi lebih tertata, sementara Group Policy Object berhasil memberlakukan kebijakan keamanan secara terpusat dan otomatis ke seluruh komputer client. Hasil Black Box Testing atas tujuh belas skenario memperlihatkan bahwa seluruh fungsi berjalan sesuai harapan, sehingga penerapan Active Directory ini terbukti mampu meningkatkan efisiensi administrasi, konsistensi konfigurasi, serta keamanan pengelolaan sumber daya IT dibandingkan sistem workgroup yang dipakai sebelumnya.

Saran

Untuk pengembangan ke depan, disarankan agar ditambahkan Backup Domain Controller demi meningkatkan ketersediaan layanan, memperluas cakupan kebijakan GPO seperti pembatasan akses internet

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

berdasarkan kategori situs dan pengaturan pembaruan sistem secara terpusat, mengintegrasikan Active Directory dengan layanan identitas modern semacam Microsoft Entra ID untuk mendukung lingkungan hibrida, menjalankan mekanisme backup dan disaster recovery secara rutin, serta melaksanakan evaluasi keamanan berkala lewat pemantauan Audit Log dan peninjauan kebijakan hak akses.

E. DAFTAR PUSTAKA

Ajrina, N. N., Febrianti, G. D., & Agussalim, A. (2024). Perancangan Desain Jaringan Dengan Konsep VLSM Menggunakan Metode PPDIOO di SMAN 1 Taman. *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *8*(2), 113. https://doi.org/10.30872/jurti.v8i2.13881

Budiyanto, V., & Herawatie, N. (2023). ANALISIS KEAMANAN SEBUAH DOMAIN MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) Zap. *Jurnal Teknologi Technoscientia*, *15*(2), 27–37. https://doi.org/10.34151/technoscientia.v15i2.4013

Harahap, H., & Handoko, D. (2024). *Pengembangan Sistem Keamanan Pusat Data*. *6*(01). https://doi.org/10.35447/jikstra.v6i1.1075711

Jumarta, A., Romegar Mair, Z., & Ramadhan, M. (2025). Implementasi Active Directory Domain Controller Pada Stasiun Meteorologi Sultan Mahmud Badaruddin Ii Palembang Untuk Pengelolaan Akses Dan Keamanan Data. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(4), 5886–5894. https://doi.org/10.36040/jati.v9i4.13910

Moch Afdal Dzikri Maulana, Arip Solehudin, C. (2026). *IMPLEMENTASI ROLE-BASED ACCESS CONTROL (RBAC) PADA ACTIVE DIRECTORY DOMAIN SERVICE UNTUK MANAJEMEN HAK AKSES PENGGUNA DI SERVER SMK AL-BADAR*. *14*(2). https://doi.org/10.23960/jitet.v14i2.9106

Muhamad, R., Nabillah, A., & Maesaroh, S. (2025). Implementasi Kebijakan Grup Policy Untuk Mitigasi Risiko Keamanan Pada Server di PT XYZ. *Jurnal Ilmiah Sains Dan Teknologi*, *9*(1), 1–9. https://doi.org/10.47080/saintek.v9i1.3912

Pratama, I. P. A. E., Andreyana, P. V., & Nurjana, P. R. (2024). Pengujian High Availability pada Asynchronous DNS Berbasis Restknot menggunakan Algoritma Round Robin. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *5*(1), 1019–1032. https://doi.org/10.35870/jimik.v5i1.582

Putri Arini, A., Raihan Ramadhani Isworo, M., Salim, A., Pembangunan Nasional, U., & Timur, J. (2021). Seminar Nasional Informatika Bela Negara (SANTIKA) Desain Dan Manajemen Jaringan Pada Sma Negeri 15 Surabaya Menggunakan Cisco Packet Tracer Dengan Metode PPDIOO. *Seminar Nasional Informatika Bela Negara (SANTIKA)*, *4*, 1–32. https://santika.upnjatim.ac.id/submissions/index.php/santika/article/view/312/173

Taberima, G. M., & Ramayanti, D. (2024). MENGOPTIMALKAN MANAJEMEN DAN KEAMANAN TI MELALUI IMPLEMENTASI LAYANAN DOMAIN ACTIVE DIRECTORY: STUDI KASUS PADA INFRASTRUKTUR TI PERUSAHAAN. *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, *6*(1), 79–89. https://doi.org/10.51401/jinteks.v6i1.3884

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)