Jurnal Informatika Teknologi dan Sains (JINTEKS)
Vol. 6 No. 1, Februari 2024, hlm. 79 – 89
ISSN 2686-3359 (Online)
EDISI 19

MENGOPTIMALKAN MANAJEMEN DAN KEAMANAN TI MELALUI IMPLEMENTASI LAYANAN DOMAIN ACTIVE DIRECTORY: STUDI KASUS PADA INFRASTRUKTUR TI PERUSAHAAN

Glen Maxie Taberima[1], Desi Ramayanti[2*]
[1,2]Teknik Informatika, Universitas Dian Nusantara
email: desi.ramayanti@undira.ac.id[2*]

Abstrak: Penelitian ini bertujuan untuk meningkatkan manajemen pengguna dan keamanan dalam infrastruktur TI sebuah perusahaan yang menghadapi kesulitan dalam mengelola jaringan yang terdiri dari 17 komputer dan 21 karyawan. Permasalahan utama terletak pada inefisiensi manajemen jaringan dan keamanan data yang tidak terpusat, yang menyebabkan peningkatan risiko keamanan dan beban kerja administratif. Metode yang digunakan adalah pendekatan PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) yang merupakan siklus pengembangan sistem menyeluruh. Melalui metode ini, penelitian ini mendemonstrasikan peningkatan dalam pengurangan insiden keamanan, manajemen terpusat, dan efisiensi operasional. Hasil utama dari penelitian ini meliputi peningkatan kontrol akses pengguna, struktur tata kelola TI yang lebih terorganisir, dan keamanan data yang lebih baik. Implementasi Layanan Active Directory Domain Services (AD DS) menyediakan manajemen yang lebih terpusat, administrasi kebijakan pengguna yang lebih efisien, dan penggunaan internet yang stabil dan aman untuk operasional bisnis sehari-hari. Kesimpulannya, AD DS menunjukkan potensi yang signifikan untuk meningkatkan praktik manajemen TI dan keamanan dalam lingkungan perusahaan. Hasil ini menyarankan bahwa organisasi lain dengan tantangan serupa dapat mempertimbangkan penerapan AD DS untuk manajemen TI dan keamanan data yang lebih baik.

Kata Kunci : *Active Directory Domain Services* (*AD DS*), PPDIOO, Tata Kelola IT, Keamanan Data, Manajemen IT

Abstract: *The research aimed to enhance user management and security within a company's IT infrastructure, which was struggling to manage a network consisting of 17 computers and 21 employees. The central problem was the inefficiency of network management and uncentralized data security, leading to increased security risks and administrative workload. The PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) approach, a comprehensive system development cycle, was employed as the research method. This approach demonstrated improvements in reducing security incidents, centralized management, and operational efficiency. The primary outcomes included better user access control, more organized IT governance structures, and improved data security. The implementation of Active Directory Domain Services (AD DS) provided more centralized management, efficient user policy administration, and stable and secure internet use for daily business operations. In conclusion, AD DS shows significant potential to improve IT management and security practices within a corporate environment. This result suggests that other organizations with similar challenges could consider implementing AD DS for better IT management and data security.*

Keywords **:** *Active Directory Domain Services (AD DS), PPDIOO, IT Governance, Data Security, IT Management*

PENDAHULUAN

Dalam era digital saat ini, pengelolaan sumber daya informasi dan keamanan data menjadi aspek kritikal yang menentukan kesuksesan operasional perusahaan. *Active Directory Domain Services (AD DS)* berperan sebagai pilar utama dalam infrastruktur IT yang modern, memfasilitasi organisasi dalam mengorganisir dan mengamankan data serta sumber dayanya secara efisien. Dengan semakin dominannya peran teknologi dalam lingkungan kerja, kebutuhan akan sistem manajemen yang terpusat dan efisien untuk mengelola pengguna dan kebijakan menjadi sangat krusial [1]. AD DS menawarkan sebuah solusi komprehensif untuk mengatasi berbagai masalah administrasi dan keamanan dengan menyediakan layanan direktori yang terstruktur dan mudah di skalakan.

Perusahaan yang menjadi fokus studi ini, dengan 21 karyawan yang tersebar di berbagai divisi, menghadapi tantangan dalam pengelolaan jaringannya, termasuk 17 unit komputer yang terkoneksi melalui *router* dan *switch* dengan alokasi alamat IP oleh protokol DHCP secara dinamis.

Tantangan utama yang diidentifikasi adalah pengelolaan kebijakan akses yang tidak terpusat, yang memungkinkan pengguna memiliki kontrol yang sama atas komputer dan *file* dalam jaringan. Hal ini tidak hanya membuka celah keamanan tapi juga meningkatkan beban kerja administratif karena pengaturan keamanan dan akses harus dikonfigurasi secara individual pada masing-masing komputer.

Penelitian dan kasus studi sebelumnya mengenai implementasi AD DS telah menunjukkan peningkatan signifikan dalam efisiensi pengelolaan jaringan, produktivitas kerja, dan kemudahan bagi admin jaringan dalam mengelola jaringan [2]. Kajian tersebut menyoroti bagaimana AD DS dapat dimanfaatkan untuk mengatur kebijakan pengguna, mengontrol akses data, dan mengamankan jaringan dari aktivitas yang tidak diinginkan [3], [4]. Melalui implementasi pembatasan akses yang lebih ketat, seperti pengaturan kebijakan kata sandi yang kuat dan pembatasan pemasangan aplikasi, risiko keamanan seperti serangan kata sandi dan *ransomware* dapat diminimalisir [5], [6].

Berdasarkan analisis tersebut, penelitian ini mengusulkan implementasi AD DS sebagai solusi

untuk memperoleh kontrol yang lebih baik atas pengguna dan sumber daya jaringan [7]. Implementasi ini diharapkan tidak hanya mengurangi insiden keamanan, seperti kata sandi yang lemah dan akses tidak sah, tetapi juga memungkinkan manajemen TI untuk mengelola kebijakan secara terpusat, mengatur hak akses sesuai dengan kebutuhan spesifik divisi, dan mengontrol instalasi aplikasi. Dengan demikian, penelitian ini bertujuan untuk mencapai tata kelola TI yang lebih efektif dan peningkatan keamanan data, sambil tetap memenuhi kebutuhan dasar penggunaan internet yang stabil dan aman untuk kegiatan bisnis sehari-hari[8], [9].

TINJAUAN PUSTAKA

Active Directory merupakan implementasi dari *Lightweight Directory Access Protocol (LDAP)* yang dikembangkan oleh Microsoft untuk sistem operasi Windows. Fungsi utamanya adalah menyediakan layanan otentikasi dan otorisasi untuk sistem operasi berbasis Windows. Selain itu, dalam *Active Directory*, seorang administrator dapat mengelola kebijakan dan mendistribusikan perangkat lunak secara luas [10], [11]. *Active Directory Domain Services (AD DS)* berperan sebagai layanan direktori yang mengandung konfigurasi jaringan, termasuk informasi tentang pengguna, grup, komputer, perangkat keras, dan kebijakan keamanan, dalam satu basis data pusat. Peran utama *Active Directory* adalah menyediakan sarana untuk mengelola administrasi jaringan secara terpusat, baik dalam satu *domain* maupun lintas *domain*, asalkan semua *domain* tersebut berada dalam satu *forest* (hutan). Tanpa keberadaan akun dalam *forest Active Directory*, akses terhadap objek dan sumber daya yang dikoneksikan melalui *Active Directory* tidak akan dimungkinkan [12]. *Forest* dalam *Active Directory* adalah komponen krusial yang mencakup *domain*, *domain tree*, skema, objek, dan *Organizational Unit* (OU), yang memungkinkan pengelolaan sumber daya dan kebijakan dengan efektif dan terorganisir.

Organizational Unit (OU) dalam *Active Directory* adalah wadah yang dapat berisi *User*, *Group*, *Computer*, dan OU lainnya, yang disusun berdasarkan departemen, divisi, fungsi kerja, proyek, dan sebagainya. Fungsionalitas OU termasuk representasi hirarki dan logika organisasi, manajemen konsisten kelompok objek, delegasi izin akses untuk administrasi kelompok objek, serta implementasi kebijakan [13].

Group Policy digunakan untuk mengatur dan menerapkan berbagai kebijakan, termasuk kebijakan keamanan. Kebijakan grup dapat diterapkan baik secara lokal pada mesin tertentu maupun melalui *Active Directory*. Untuk meninjau pengaturan kebijakan grup yang berlaku secara lokal pada sistem, pengguna dapat menjalankan program gpedit.msc sebagai *administrator*, yang dapat diakses melalui baris perintah atau kotak *run*. Kebijakan grup dapat dikonfigurasi pada berbagai tingkatan, termasuk kebijakan grup lokal, kebijakan yang terkait dengan situs, *domain*, dan OU. Umumnya, disarankan untuk mengelola kebijakan grup pada tingkat situs, *domain*, atau OU untuk menghindari perlunya replikasi manual pada setiap mesin dan memanfaatkan kemampuan *Active Directory* dalam mengelola banyak sistem secara bersamaan [14].

Windows Server adalah sistem operasi *server* yang dirancang oleh Microsoft, dengan fokus utama pada manajemen pengguna dan grup, bertujuan untuk memberikan hak akses yang sesuai dan mengelola berbagai sumberdaya jaringan untuk pengguna [5]. Akun pengguna digunakan sebagai cara untuk masuk ke dalam jaringan *domain* Windows. Terdapat dua jenis akun pengguna berdasarkan jangkauannya: *Local User Account*, yang terbatas pada satu komputer dan hanya dapat digunakan untuk masuk ke komputer tempat akun dibuat; dan *Domain User Account*, yang berlaku di seluruh domain dan dibuat melalui layanan *Active Directory* di *Domain Controller*.

METODE

Metodologi *Prepare, Plan, Design, Implement, Operate, Optimize* (PPDIOO) adalah pendekatan menyeluruh yang diterapkan dalam proyek-proyek manajemen jaringan dan teknologi informasi (TI), termasuk dalam penerapan *Active Directory Domain Services* (AD DS). Pendekatan ini dirancang untuk memastikan bahwa implementasi berjalan secara terstruktur, efektif, dan berorientasi pada kebutuhan bisnis serta pengguna [15]. Tahapan "*Prepare*" melibatkan pengumpulan persyaratan awal dan tujuan proyek, sementara "*Plan*" fokus pada pengembangan strategi rinci untuk mencapai tujuan tersebut. Tahap "*Design*" merinci arsitektur dan solusi yang akan diimplementasikan. Selanjutnya, "*Implement*" menyangkut penerapan desain ke dalam lingkungan produksi. "*Operate*" mengacu pada pengelolaan sistem yang telah diterapkan, dan "*Optimize*" berfokus pada peningkatan berkelanjutan untuk meningkatkan efisiensi dan kinerja sistem.

Gambar 1. Metode PPDIOO

Prepare: Pada tahapan ini dilakukan analisis kebutuhan melalui wawancara dan observasi yang mengungkapkan kebutuhan penting seperti kemampuan pemulihan kata sandi yang lebih baik, pembagian file yang aman antar divisi, pembatasan

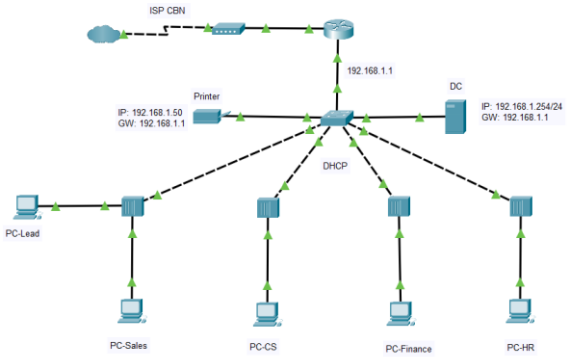
ISSN 2686-3359 (Online)
EDISI 19

aplikasi yang tidak terkait pekerjaan, serta peningkatan keamanan dan efisiensi [16]. Ditemukan juga bahwa manajemen jaringan yang terpusat dan peningkatan alokasi *IP* serta stabilitas koneksi internet menjadi sangat penting [17]. Oleh karena itu, disarankan untuk mengadopsi *Active Directory Domain Services (AD DS)* untuk pengelolaan pusat, kontrol akses yang lebih baik, pemulihan kata sandi yang mudah, dan pemantauan aktivitas secara *real-time*, mendukung ekspansi dan kebutuhan yang berkembang dari perusahaan. Implementasi ini bertujuan untuk memperkuat keamanan, mengsentralisasi manajemen jaringan, meningkatkan efisiensi melalui otomatisasi, dan mengembangkan infrastruktur yang dapat disesuaikan, lengkap dengan program pelatihan untuk staf. Saat ini, infrastruktur jaringan yang terdiri dari perangkat standar dan Windows 10 tanpa pengelolaan *server* pusat, meskipun berkinerja cukup baik, tetapi membatasi efektivitas pengelolaan sumber daya. Migrasi ke AD DS diharapkan memungkinkan pengelolaan yang terpusat, penerapan kebijakan keamanan yang seragam, peningkatan perangkat keras, serta pelatihan staf, yang ke semuanya akan meningkatkan keamanan, manajemen, dan efisiensi operasional secara keseluruhan.

Plan: Dalam langkah perencanaan yang ditetapkan untuk sembilan minggu, rencana proyek yang detail disiapkan untuk mengarahkan tahapan dari awal pengenalan kebutuhan bisnis hingga fase evaluasi sistem, memastikan bahwa seluruh proses dilaksanakan dengan efisien dan sistematis. Kebutuhan dasar seperti penggunaan Kabel UTP untuk koneksi jaringan, sebuah PC yang akan ditugaskan sebagai *server* dengan sistem operasi yang sesuai, serta seorang *administrator* yang diberikan wewenang penuh untuk menyesuaikan kebijakan dan konfigurasi *server* telah diidentifikasi dan siap digunakan. Menyusul persiapan ini, fokus bergeser ke strategi migrasi yang cermat, yang melibatkan langkah-langkah penting seperti mem-*backup* data kritis ke *harddisk* eksternal untuk kemudian dipulihkan ke komputer setelah mereka sukses terintegrasi ke dalam *domain* AD DS. Sebuah *server* dengan alamat *IP* 192.168.1.254 akan ditambahkan, sesuai dengan konfigurasi jaringan yang telah ada dan menggunakan *IP gateway router* di 192.168.1.1, sementara klien akan diberi *IP* dinamis dalam rentang 192.168.1.10 hingga 192.168.1.100 dengan *prefix* /24, memastikan transisi yang mulus ke dalam *setup* jaringan yang telah terestablis.

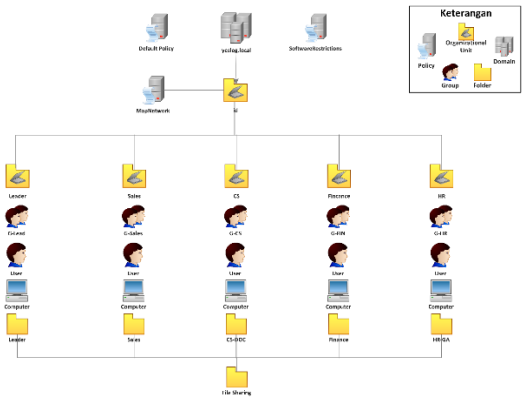
Design: Tahap desain infrastruktur melibatkan pengembangan rancangan *Local Area Network (LAN)* yang terstruktur dalam satu *subnet*, seperti yang diilustrasikan dalam desain topologi perusahaan pada Gambar 2. Rencana ini mencakup

penempatan satu *server Domain Controller (DC)* yang akan menyediakan layanan *DNS Server*, *Active Directory*, dan *File Server*, dengan pembagian alamat *IP* yang otomatis kepada semua klien melalui protokol *DHCP* dari *router*.



Gambar 2. Desain Topologi Perusahaan

Dalam pembentukan struktur *Organizational Unit (OU)* di *domain* perusahaan, pembagian dibuat sesuai dengan divisi-divisi yang ada, dan setiap OU akan diberikan *group policy* khusus baik di tingkat *domain* maupun OU itu sendiri untuk mengendalikan kebijakan secara keseluruhan. Struktur OU ini dirancang untuk mencakup lima OU yang masing-masing mewakili divisi dalam perusahaan, di mana setiap OU berisi grup, pengguna, komputer, dan *folder* untuk keperluan berbagi *file* antar divisi atau pengguna. Keamanan jaringan diatur melalui *Group Policy Object (GPO)* yang terbagi dalam tiga kategori utama: pengaturan global, pembatasan aplikasi, dan kebijakan berbagi jaringan.



Gambar 3. Perancangan *Organization Unit (OU)*

Fokus pada keamanan *server*, terutama *server* yang berfungsi sebagai *Active Directory*, menjadi prioritas utama dengan langkah-langkah perlindungan dan pemantauan keamanan yang ketat [18]. Ini termasuk pembuatan partisi baru untuk *log* sistem yang terpisah, memungkinkan penyimpanan *log* aplikasi, keamanan, dan sistem dengan ekstensi evtx di lokasi yang aman dengan akses terbatas hanya untuk *Administrator* seperti pada Tabel 1. Kebijakan *audit* diaktifkan untuk memantau aktivitas yang mencurigakan di *server* dan *workstation* (Tabel 2), mencatat baik keberhasilan maupun kegagalan dalam berbagai sub kategori aktivitas pengguna dan sistem [19].

ISSN 2686-3359 (Online)
EDISI 19

Tabel 1. Perubahan *Path log*

Path	Hak Akses
E:\Logs\Application	*Domain Admin*
E:\Logs\Security	
E:\Logs\System	

Tabel 2. Kebijakan Audit

Kategori	Sub Kategori	*Success*	*Failure*
Account Logon	*Credential Validation*	*Y*	*Y*
	Kerberos Auth Service	*Y*	*Y*
	Kerberos Service Ticket Operations	*Y*	*Y*
	Other Account Logon Events	*Y*	*Y*
Account Management	*Computer Account Management*	*Y*	*Y*
	Other Account Management Events	*Y*	*Y*
	Security Group Management	*Y*	*Y*
	User Account Management	*Y*	*Y*
Detailed Tracking	*DPAPI Activity*	*Y*	*Y*
	Process Creation	*Y*	*Y*
DS Access	*Directory Services Access*	*Y*	*Y*
	Directory Services Changes	*Y*	*Y*
Logon and Logoff	*Account Lockout*	*Y*	*N*
	Logoff	*Y*	*N*
	Logon	*Y*	*Y*
	Other Logon/Logoff Events	*Y*	*Y*
	Special Logon	*Y*	*Y*
Policy Change	*Policy Change*	*Y*	*Y*
	Auth Policy Change	*Y*	*Y*
	MPSSVC Rule-Level Policy Change	*Y*	
System	*IPsec Driver*	*Y*	*Y*
	Security State Change Events	*Y*	*Y*
	Security System Extension	*Y*	*Y*
	System Integrity	*Y*	*Y*

Kebijakan pembuatan kata sandi dirancang untuk meningkatkan keamanan dengan menetapkan persyaratan minimum panjang kata sandi 10 karakter yang mencakup kombinasi huruf besar, huruf kecil, angka, dan karakter khusus. Sistem juga akan membatasi kesalahan login hingga tiga kali sebelum mengunci akun selama 30 menit, dengan perubahan kata sandi yang diperlukan setiap 30 hari untuk menjaga integritas akun pengguna.

Group Policy diimplementasikan dengan spesifikasi tertentu untuk setiap *level* (Tabel 3), dari *Default Policy* di tingkat *domain* hingga kebijakan khusus seperti *MapNetwork* dan *SoftwareRestrictions* pada *level* OU, menargetkan pembatasan instalasi aplikasi dan pembuatan *drive* jaringan otomatis yang tersedia untuk semua klien di OU tertentu.

Tabel 3. *Group Policy*

Level	*Group Policy*
Domain	*Default Policy*
	SoftwareRestrictions
	Audit
OU	*MapNetwork*

Pembagian hak akses untuk berbagi *file* diatur melalui grup pada setiap OU, dengan setiap folder dinamakan sesuai divisi dan dibagi menjadi subfolder Publik dan Privat, di mana hak akses ditentukan berdasarkan kebutuhan dan kewenangan divisi (Tabel 4). Proses ini memastikan bahwa setiap divisi memiliki kontrol dan privasi atas *file* dan *folder* mereka, dengan *Administrator* memiliki kontrol penuh atas manajemen direktori keseluruhan.

Tabel 5. Hak Akses *Folder*

Folder	***Lead***		***Sales***		***CS***		***Fin***		***HR***	
G/U	***PB***	***PV***	***PB***	***PV***	***PB***	***PV***	***PB***	***PV***	***PB***	***PV***
Lead	*RW*	*RW*	*R*		*R*		*R*		*R*	
Sales	*R*		*RW*	*RW*	*R*		*R*		*R*	
CS	*R*		*R*		*RW*	*RW*	*R*		*R*	
Fin	*R*		*R*		*R*		*RW*	*RW*	*R*	
HR	*R*		*R*		*R*		*R*		*RW*	*RW*

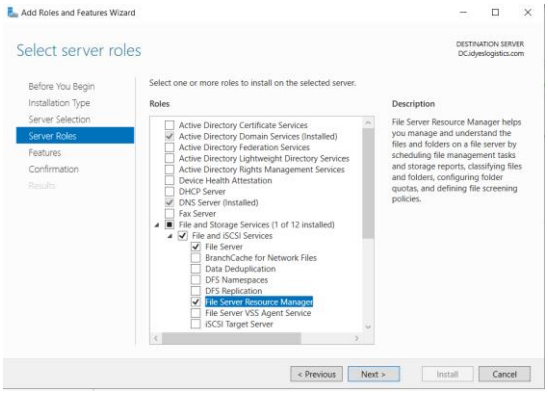
KETERANGAN:
PB = Public, PR = Private
RW = Read/Write, R = Read, W = Write

Implement: Tahap implementasi merupakan bagian krusial dalam penerapan AD DS, di mana langkah-langkah penting diambil berdasarkan desain yang telah dirumuskan, termasuk pemasangan AD DS dan verifikasi jaringan serta keamanan untuk memastikan semua berfungsi sesuai dengan standar yang ditentukan. Proses ini dimulai dengan pemasangan dan konfigurasi *Active Directory* pada *server*, yang dilaksanakan setelah sistem operasi Windows Server 2019 berhasil dipasang. Ini melibatkan penyiapan *server* dengan peran AD DS, pengaturan kebijakan keamanan, dan konfigurasi layanan DNS yang diperlukan untuk mendukung fungsi pencarian nama dalam jaringan.

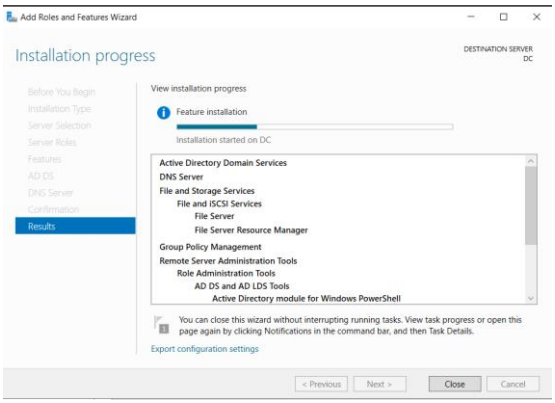
ISSN 2686-3359 (Online)
EDISI 19

Server Roles

Pada *server* dibuat penentuan *Role* yang akan digunakan dengan memilih *Active Directory Domain Services, DNS Server, dan File Server* seperti pada Gambar 4 dan 5. Setelah instalasi selesai, *server* akan di *promote* menjadi *Active Directory*. *Server* akan menjadi sebuah *domain* baru yang juga merupakan *forest* baru dalam jaringan. *Domain* yang digunakan adalah "*yeslog.local*" dan *NetBios Name* adalah YESLOG.*



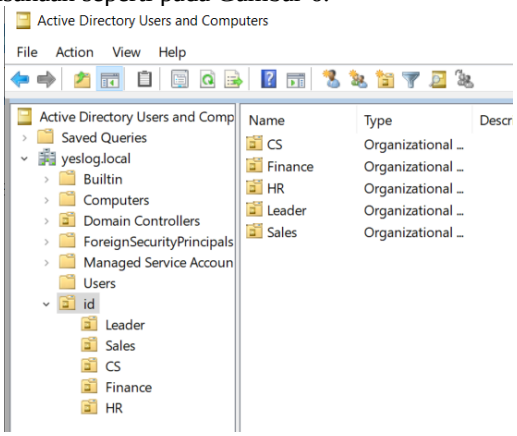
Gambar 4. Pemilihan *Server Roles*



Gambar 5. Proses *Instalasi Roles Server* yang telah dipilih sebelumnya

Organization Unit

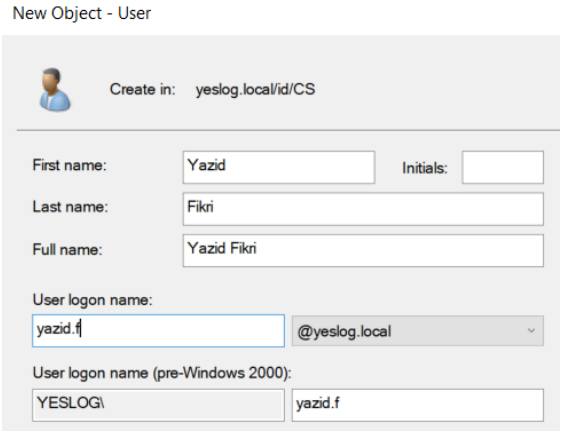
Organization Unit (OU) dibuat pada *domain* dengan menggunakan *tool AD User & computer* dengan berdasar pada divisi yang ada pada perusahaan seperti pada Gambar 6.



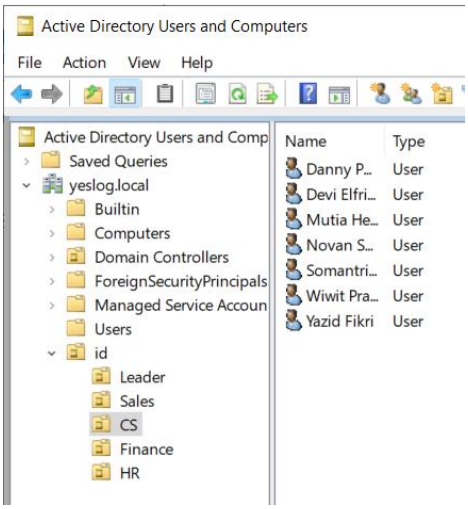
Gambar 6. Pembuatan Organization Unit

User dan *Group*

User dibuat pada setiap OU yang telah dibuat sebelumnya menggunakan *tool AD User & Computer*. Kemudian diisi *first name, Last Name,* dan *User Logon name*. Pada *user logon name*, diisi dengan *format first name.inisial last name* seperti pada Gambar 7, sehingga daftar *user* akan terlihat seperti salah satu divisi yang dibuat pada Gambar 8. Cara tersebut mewakili teknik pembuatan *user* setiap divisi secara keseluruhan.



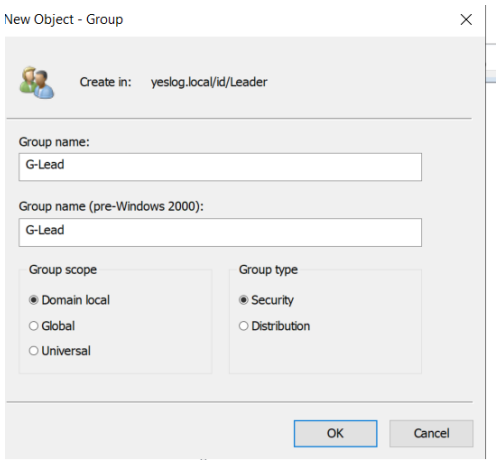
Gambar 7. Proses Pembuatan *User*



Gambar 8. Pembuatan *User*

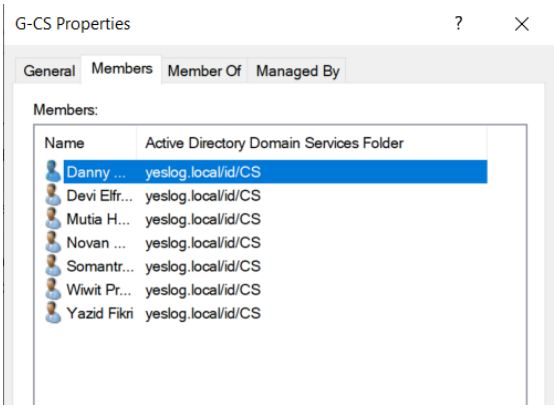
Konfigurasi Grup dibuat menggunakan *tool AD Users & Computer* juga dengan mengisi nama grup seperti pada tahap perancangan. *Scope* ditentukan untuk *local domain* dan *Type* pada bagian *security* seperti pada Gambar 8.

ISSN 2686-3359 (Online)
EDISI 19



Gambar 9. Pembuatan Grup

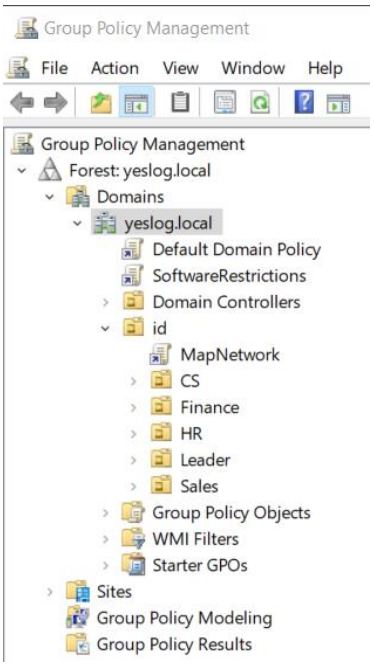
Setelah pembuatan grup selesai, dilanjutkan dengan menentukan member yaitu *user* sebagai bagian dari grup masing-masing divisi seperti pada Gambar 10 agar mudah diterapkan sebuah aturan secara menyeluruh kepada seluruh *user*.



Gambar 10. Penambahan *Member Group*

Group Policy

Untuk menerapkan kebijakan pembatasan perangkat lunak pada sistem Windows, langkah-langkahnya dilakukan dengan membuat *script* baru yaitu *MapNetwork*, *SoftwareRestrictions*, *Password*, dan *Audit*. Konfigurasi dilakukan dengan membuka *edit Group Policy Objek (GPO)* dan mengkonfigurasi masing-masing *script* untuk pengaturan *policy*.



Gambar 11. Tampilan *Group Policy Management*

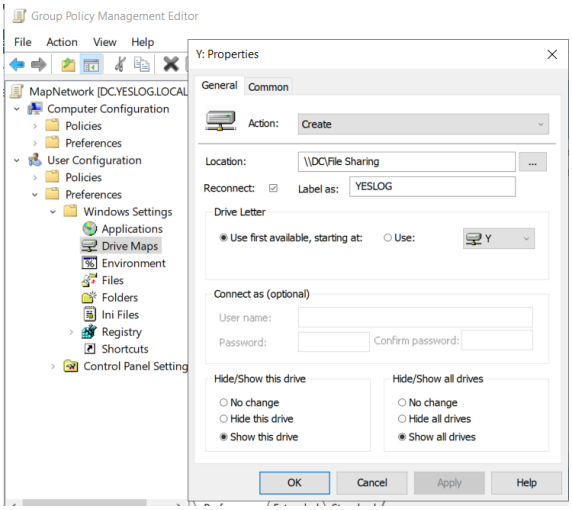
Password Policy

Pembuatan kebijakan pengaturan *password* dengan aturan panjang kata sandi 10 karakter dengan menerapkan *complexity* seperti ada angka, simbol, *uppercase*, *lowercase*, dan *special character*. Dalam 30 hari, kata sandi akan di *reset* dan harus diubah oleh masing-masing komputer. jika terdapat salah inputan kata sandi, akun akan terkunci dalam waktu 1 jam bilamana *password* yang dimasukkan mencapai kesalahan 3 kali. Akun yang terkunci hanya bisa dibuka oleh *Administrator* sehingga pengguna wajib menghubungi *Administrator* untuk mengatasi masalah tersebut. Kompleksitas, panjang, periode *valid*, dan lainnya perlu diterapkan dengan terus memperbarui kata sandi yang memiliki kemungkinan dibobol dengan menerapkan pelatihan terhadap kesadaran keamanan dan pemilihan kata sandi yang tepat [19].

Drive Maps

Drive Maps dibuat melalui *Group Policy Management Editor* pada *script* MapNetwork dengan masuk pada user *configuration*, *folder preferences*, *windows settings*, dan pilih *Drive Maps* kemudian membuat *Location* yang menuju ke *folder* yang telah dibuat pada *server* bernama *"File Sharing"* dengan *path \\DC\\File Sharing* dengan merubah *Label* menjadi YESLOG dan menentukan *Drive Letter Y* seperti pada Gambar 12.

ISSN 2686-3359 (Online)
EDISI 19



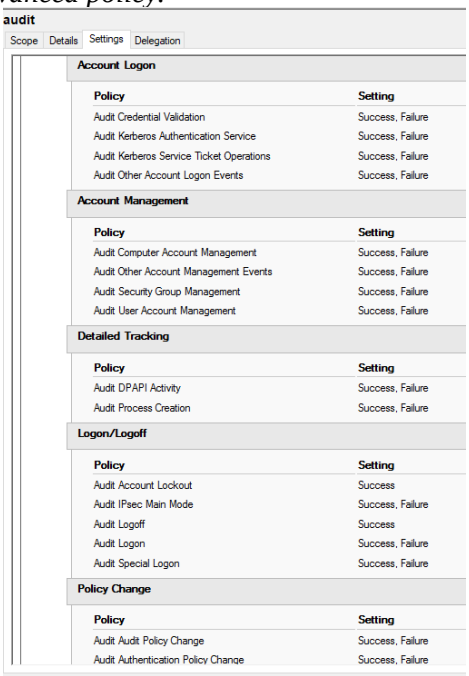
Gambar 12. Pengaturan *Drive Maps*

Software Restriction

Tahap ini dilakukan dengan masuk ke GPO dengan mengakses *Software Restriction Policies* pada *computer configuration*. Kemudian menambahkan kebijakan baru dan mengatur tingkatan keamanan. Setelah itu menentukan *File type* berekstensi *exe* dan *msi* untuk menerapkan pembatasan pada jenis *file* tersebut dan memberikan pengecualian terhadap *libraries*.

Audit

Pengaturan dibuat pada GPO dengan mengkonfigurasi peraturan komputer pada *local & advanced policy.*



Gambar 13. *Setting* GPO untuk *audit*

Hak Akses File & Folder

Pada masing-masing folder dibuat pengaturan *security* dengan menentukan hak akses pada setiap user melalui fungsi grup yang telah ditentukan pada AD. *Subfolder* yang merupakan *Parent Folder* dari Nama Setiap divisi, ditentukan hak akses grup pada subfolder *Public & Private*. *Folder Public* diberi akses kepada seluruh user dengan hak akses *Read* dan pada *Private folder* diberi akses hanya untuk divisi tertentu yang memiliki akses ke folder tersebut. Dalam hal hak akses secara keseluruhan, Administrator memiliki otoritas sepenuhnya untuk mengelola semua direktori di setiap bagian.

HASIL DAN PEMBAHASAN

Prepare

Identifikasi kebutuhan TI perusahaan melalui wawancara dan observasi yang menghasilkan keputusan untuk mengadopsi AD DS. Inisiatif ini bertujuan untuk mengatasi tantangan manajemen jaringan terpusat, alokasi IP, dan stabilitas koneksi internet.

Plan

Penyusunan rencana proyek sembilan minggu mencakup persiapan infrastruktur, pemilihan perangkat keras, dan strategi migrasi data.

Design

Pengembangan rancangan LAN dalam satu subnet dengan pembagian alamat IP otomatis dan pembentukan struktur OU yang mencerminkan divisi-divisi perusahaan, dilengkapi dengan kebijakan grup yang sesuai.

Implementation

Pemasangan dan konfigurasi AD DS dan DNS pada server, diikuti dengan integrasi klien dan penerapan kebijakan grup termasuk pembatasan perangkat lunak dan kebijakan kata sandi.

Testing and Validation

Dilakukan pemeriksa fungsi jaringan dan keamanan untuk memastikan bahwa semua fungsi berjalan sesuai dengan pengaturan. Pada proses pengujian dan validasi dilakukan sesuai dengan skenario yang ditentukan pada tabel dan hasil yang menyatakan bahwa semua konfigurasi berfungsi sesuai dengan keinginan.

Tabel 6. Hasil Pengujian dan Validasi

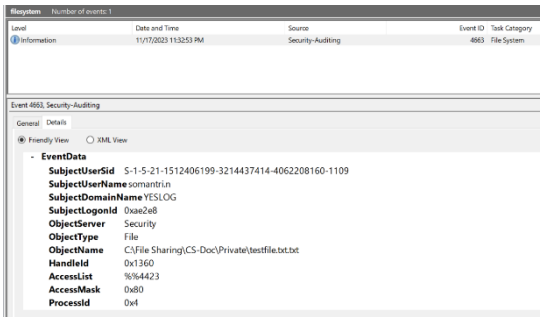
Skenario	Deskripsi	Langkah Pengujian	Hasil
Join Domain	Memastikan *device* dapat	Bergabung ke *domain* dengan	Perangkat berhasil

	join ke *domain*	perangkat baru	bergabung ke *domain*
Autentikasi dan Otorisasi	Memastikan pengguna dapat *login* & mendapat akses	Pengujian *login* *domain*, Verifikasi hak akses	Autentikasi keberhasil, akses sesuai dengan peran
Kebijakan Kata Sandi	Menguji implementasi kebijakan kata sandi	Penerapan kebijakan kata sandi baru, Menguji *Reset* Kata Sandi	Kebijakan & *Reset* Kata sandi Berhasil
File Sharing & Akses *Folder*	Menguji hak akses terhadap *file* dan *folder* *sharing*	Pembagian *File* & *Folder*, Verifikasi hak akses	Akses *file* & *folder* sesuai dengan kebijakan
Izin pemasangan aplikasi	Memastikan izin instalasi aplikasi terkendali	Uji instalasi di komputer	Instalasi aplikasi sesuai aturan
Keamanan Jaringan dan *Audit Log*	Uji penetrasi & pemeriksaan *log aktivitas*	Uji penetrasi menggunakan *tool* *Responder* & *Hashcat*, Pemeriksaan *log* aktivitas	Aktivitas tercatat dengan baik.

Operate

Pada tahap kelima dari metode PPDIOO yaitu operasional, dilakukan *monitoring* yang bertujuan untuk mengawasi kinerja jaringan untuk memastikan keamanan jaringan dan berjalan sesuai dengan pengaturan. Pada proses ini dilakukan dengan *tools event viewer* untuk melihat setiap kejadian yang terjadi dalam jaringan. Salah satu metode melibatkan *audit* keamanan, yang bertujuan untuk memahami aktivitas yang dilakukan oleh pengguna yang mempunyai hak akses terhadap *folder* atau *file* yang dibagikan ke seluruh divisi.

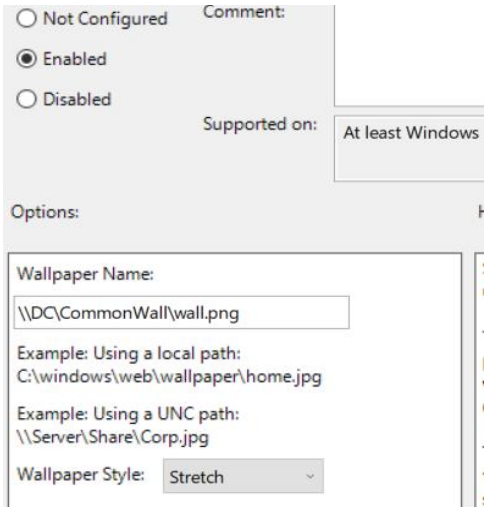
Seperti pada gambar 14, diketahui bahwa sebuah *file* baru dibuat dalam *Folder* milik divisi CS yaitu file berekstensi txt. Petunjuk ini tidak berpengaruh terhadap tindakan "*DELETE*" karena hak *delete* dinonaktifkan sehingga untuk perilaku lain dapat diketahui.



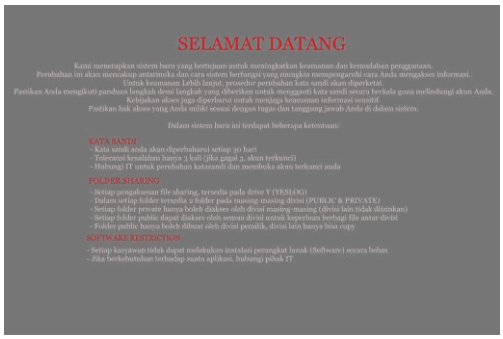
Gambar 14. Tampilan Proses *Audit*

Pelatihan

Pelatihan dan pengenalan sistem baru kepada pengguna dilakukan melalui metode kreatif dengan memanfaatkan wallpaper pada setiap komputer. Informasi penting seperti prosedur perubahan kata sandi dan kebijakan akses disampaikan melalui wallpaper ini. Implementasi wallpaper dilakukan dengan menambahkan *script* pada *Group Policy Object (GPO)*, memastikan informasi cepat tersebar dan diterima oleh semua karyawan dalam jaringan. Metode ini efektif untuk memastikan pengguna memahami dan mengikuti prosedur sistem baru dengan cepat dan efisien.



Gambar 15. Pengaturan GPO untuk penyebaran informasi melalui *wallpaper*



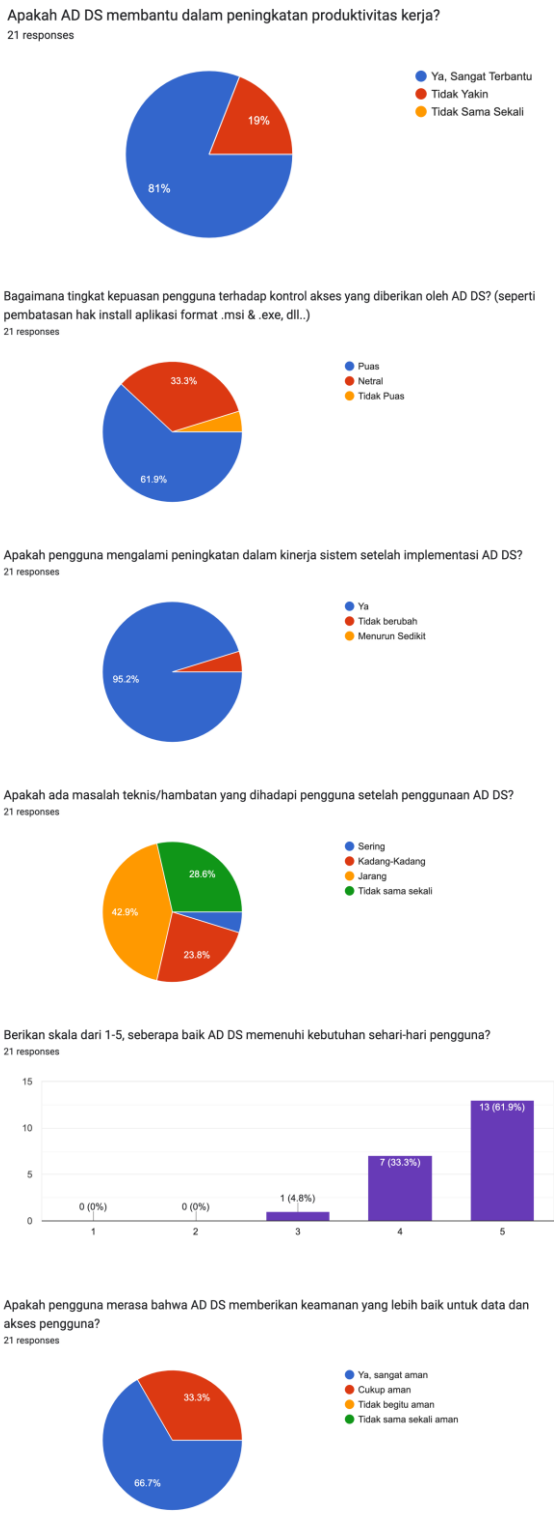
Gambar 16. *Wallpaper* yang dijadikan sebagai media informasi

Optimize

Tahap Optimasi dalam metodologi PPDIOO adalah langkah penting untuk mengevaluasi kinerja sistem yang telah diimplementasikan dan untuk meningkatkan kualitas jaringan perusahaan. Pada tahap ini, digunakan dua alat utama, yaitu "iperf" untuk pengujian kinerja jaringan dan kuesioner untuk mengumpulkan umpan balik pengguna.

Hasil evaluasi menunjukkan bahwa implementasi AD DS telah memberikan kepuasan tinggi kepada pengguna. Sebagian besar pengguna melaporkan peningkatan dalam kinerja sistem dan merasa bahwa keamanan data telah ditingkatkan. Meskipun ada beberapa masalah teknis yang dihadapi pengguna, evaluasi secara keseluruhan mengindikasikan bahwa AD DS efektif memenuhi kebutuhan pengguna dan meningkatkan kepercayaan terhadap keamanan data perusahaan.

Dalam rangka mengumpulkan masukan yang relevan, telah dilakukan penyebaran kuesioner kepada 21 responden yang berpartisipasi dalam penggunaan *Active Directory Domain Services (AD DS)*. Kuesioner ini terdiri dari 8 pertanyaan yang merangkum berbagai aspek penggunaan AD DS. Pertama, pengguna diminta untuk menilai tingkat kemudahan dalam menavigasi dan menggunakan sistem baru ini. Selanjutnya, mereka diminta untuk mengevaluasi dampak AD DS terhadap peningkatan produktivitas kerja mereka. Aspek kontrol akses juga dievaluasi, dengan pertanyaan mengenai tingkat kepuasan terhadap pembatasan hak instalasi aplikasi *format* .msi & .exe, serta masalah teknis yang mungkin dihadapi. Pengguna juga diberi kesempatan untuk memberikan saran atau masukan tambahan terkait sistem. Selain itu, mereka diminta untuk memberikan penilaian dari 1 hingga 5 terkait sejauh mana AD DS memenuhi kebutuhan sehari-hari, dengan 1 sebagai tidak memuaskan dan 5 sebagai sangat memuaskan. Terakhir, pandangan pengguna tentang tingkat keamanan yang diberikan oleh AD DS terhadap data dan akses pengguna juga diungkapkan. Kuesioner ini menjadi alat yang berharga dalam mengevaluasi keberhasilan implementasi AD DS dan mengidentifikasi area-area yang perlu perbaikan untuk mendukung kepuasan pengguna.



Gambar 17. *Hasil Kuesioner*

Hasil evaluasi dari pengguna terhadap sistem baru ini menunjukkan tingkat kepuasan yang positif. Sebanyak 61,9% pengguna menganggap sistem tersebut mudah digunakan, sementara 81% pengguna merasa bahwa AD DS membantu meningkatkan produktivitas kerja mereka. Aspek kontrol akses pada sistem baru juga dinilai memuaskan oleh 61,9% pengguna, dan sebanyak 95,2% pengguna

melaporkan adanya peningkatan kinerja sistem setelah implementasi AD DS.

Dalam hal masalah teknis, hanya 42,9% pengguna yang mengalami masalah secara jarang, dan 28,6% pengguna tidak mengalami masalah terkait penggunaan AD DS. Meskipun sebagian besar pengguna memberikan masukan yang mendapat nilai rendah dalam pengembangan sistem, mereka sebagian besar merasa bahwa AD DS dapat memenuhi kebutuhan sehari-hari mereka dengan nilai 61,9% pada skala 1-5. Selanjutnya, sebanyak 66,7% pengguna menyatakan bahwa tingkat keamanan sistem terjamin, mengindikasikan bahwa sistem memberikan tingkat kepercayaan yang tinggi terkait keamanan data dan informasi.

KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini menunjukkan bahwa penerapan *Active Directory Domain Services* (*AD DS*) secara efektif mendukung sentralisasi pengguna dan pengelolaan kebijakan dalam lingkungan kerja. Hasil implementasi menunjukkan peningkatan signifikan dalam efisiensi operasional, keamanan data, dan produktivitas kerja. Dengan pengelolaan yang terpusat, perusahaan dapat mengurangi insiden keamanan, meningkatkan kontrol atas sumber daya jaringan, dan memenuhi kebutuhan dasar penggunaan *internet* yang stabil dan aman untuk kegiatan bisnis. Evaluasi pengguna menunjukkan tingkat kepuasan yang tinggi, menegaskan bahwa AD DS memenuhi ekspektasi dalam memperkuat keamanan dan meningkatkan kinerja sistem. Saran untuk penelitian selanjutnya termasuk eksplorasi strategi optimasi lanjutan untuk meningkatkan efektivitas AD DS dalam lingkungan yang dinamis dan beragam.

Saran

Untuk organisasi yang mempertimbangkan penerapan AD DS, disarankan untuk melakukan perencanaan dan persiapan yang matang, meliputi analisis kebutuhan sistem, desain infrastruktur jaringan, dan pelatihan untuk *administrator* sistem. Penelitian lebih lanjut juga diperlukan untuk mengexplore potensi AD DS dalam menghadapi tantangan keamanan data yang terus berkembang, serta mengintegrasikan solusi dengan teknologi *cloud* dan *mobile* untuk mendukung fleksibilitas kerja.

DAFTAR PUSTAKA

[1] S. Pocarovsky, M. Koppl, And M. Orgon, "Security Test Of Active Directory Domain Services," *Research & Development In Material Science*, Vol. 18, No. 3, Mar. 2023, Doi: 10.31031/Rdms.2023.18.000939.

[2] A. W. Firmansyah, R. D. Marcus, A. S. Ilmananda, And F. Y. Pamuji, "Manajemen Akun Pengguna Berbasis Roaming Profile Untuk Memperkuat Perlindungan Data Di Laboratorium Komputer," *Smatika Jurnal*, Vol. 12, No. 02, Pp. 255–264, Dec. 2022, Doi: 10.32664/Smatika.V12i02.688.

[3] B. Pangaribuan And Haeruddin, "Perancangan Dan Implementasi Active Directory Domain Controller Menggunakan Windows Server 2012 R2 Di Pt. Flextronics Technology Indonesia," *Oktal : Jurnal Ilmu Komputer Dan Sains*, Vol. 3, No. 1, Oct. 2021, Accessed: Nov. 05, 2023. [Online]. Available: Https://Garuda.Kemdikbud.Go.Id/Documents/Detail/2313934

[4] J. L. Rizky And P. Astuti, "Implementasi Active Directory Menggunakan Server On Premises Untuk Mengatur Rules Pengguna Data Pada Pt. Rajawali Berdikari Indonesia," *Reputasi: Jurnal Rekayasa Perangkat Lunak*, Vol. 3, No. 2022, Nov. 2022, Doi: Https://Doi.Org/10.31294/Reputasi.V3i2.1587.

[5] N. Sadikin And M. Sari, "Implementasi Password Policy Pada Domain Security Policy Group Policy Object (Gpo) Active Directory Domain Services Untuk Keamanan Jaringan Di Windows Server," *Jurnal Maklumatika*, Vol. 10, No. 1, Pp. 1–9, Jan. 2023, Accessed: Nov. 05, 2023. [Online]. Available: Https://Maklumatika.I-Tech.Ac.Id/Index.Php/Maklumatika/Article/View/152

[6] G. Mcdonald, P. Papadopoulos, N. Pitropakis, J. Ahmad, And W. J. Buchanan, "Ransomware: Analysing The Impact On Windows Active Directory Domain Services," *Sensors*, Vol. 22, No. 3, P. 953, Jan. 2022, Doi: 10.3390/S22030953.

[7] B. I. Mokhtar, A. D. Jurcut, M. S. Elsayed, And M. A. Azer, "Active Directory Attacks—Steps, Types, And Signatures," *Electronics (Basel)*, Vol. 11, No. 16, P. 2629, Aug. 2022, Doi: 10.3390/Electronics11162629.

[8] A. R. Ruli, "Implementasi Active Directory Singgle Domain Pada Anak Perusahan Akita Jaya Mobilindo Jakarta," *Prosiding Seminar Nasional Teknoka*, Vol. 2, Pp. I103–I108, Nov. 2017, Accessed: Jan. 28, 2024. [Online]. Available: Https://Journal.Uhamka.Ac.Id/Index.Php/Teknoka/Article/View/766

[9] N. Afif, "Manajemen Akses Dan Direktori User Dalam Laboratorium Ti Uin Alauddin Makassar Berbasis Active Directory Windows," *Instek: Informatika Sains Dan Teknologi*, Vol. 1, No. 1, Oct. 2016, Doi: Doi.Org/10.24252/Instek.V1i1.2544.

[10] H. Kusuma And M. A. Adiguna, "Implementasi Active Directory Domain Services Windows Server 2012 Menggunakan Virtualisasi Hypervisor Vmware Esxi (Study Kasus Pt-Etrans)," *Jupik : Jurnal Penelitian Ilmu Komputer*, Vol. 1, No. 3, Sep. 2023, Accessed: Nov. 05, 2023. [Online]. Available: Https://Mypublikasi.Com/Index.Php/Jupik/Article/View/34

[11] F. G. N. Larosa, "Implementasi Active Directory Pada Jaringan Komputer Pkmi 1 Medan," *Methodika: Jurnal Teknik Informatika Dan Sistem Informasi*, Vol. 1, No. 1, Pp. 10–21, 2015, Doi: Https://Doi.Org/10.46880/Mtk.V1i1.9.

[12] G. Grillenmeier, "Improving Your Active Directory Security Posture: Adminsdholder To The Rescue," *Cyber Security: A Peer-Reviewed Journal*, Vol. 6, No. 3, Pp. 242–260, Jan. 2023.

[13] D. Francis, *Mastering Active Directory: Design, Deploy, And Protect Active Directory Domain Services For Windows Server 2022*, 3rd Ed., Vol. 3. Birmingham: Packt Publishing Ltd, 2021.

[14] M. O'leary, "Active Directory," In *Cyber Operations: Building, Defending, And Attacking Modern Computer Networks*, M. O'leary, Ed., Berkeley, Ca: Apress, 2019, Pp. 235–275. Doi: 10.1007/978-1-4842-4294-0_6.

[15] I. M. Widiarta, S. Esabella, And P. Widiantara, "Analisis Model Pengembangan Infrastruktur Jaringan Komputer Pada Universitas Teknologi Sumbawa Sebagai Inovasi Menggunakan Metode Ppdioo," *Jurnal Tambora*, Vol. 4, No. 2a, Jul. 2020, Doi: Doi.Org/10.36761/Jt.V4i2a.780.

[16] A. Mustofa And D. Ramayanti, "Implementasi Load Balancing Dan Failover To Device Mikrotik Router Menggunakan Metode Nth (Studi Kasus : Pt. Go-Jek Indonesia)," *Jurnal Teknologi Informasi Dan Ilmu Komputer*, Vol. 7, No. 1, Pp. 139–144, Jan. 2020, Doi: 10.25126/Jtiik.202071638.

[17] D. Tanjung And H. Haerudin, "Implementasi File Server Terintegrasi Dengan Active Directory Pada Smp Bani Taqwa Kota Bekasi," *Oktal : Jurnal Ilmu Komputer Dan Science* , Vol. 1, No. 7, Pp. 986–996, Jul. 2022, Accessed: Nov. 05, 2023. [Online]. Available: Https://Journal.Mediapublikasi.Id/Index.Php/Oktal/Article/View/405

[18] M. Sabri Elmastaş, "Journal Of Aeronautics And Space Technologies 16(2) (2023) 36-55 Detection Of Current Attacks In Active Directory Environment With Log Correlation Methods Aktif Dizin Ortamındaki Güncel Saldırıların Log Korelasyon Yöntemleri Ile Tespiti."

[19] P. Sotirios And K. Labrinoudakis, "Windows Active Directory Security Audit," Master Thesis, University Of Piraeus, Greece, 2021. Doi: Dx.Doi.Org/10.26267/Unipi_Dione/964.