JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 2, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i2.9106

IMPLEMENTASI ROLE-BASED ACCESS CONTROL (RBAC) PADA ACTIVE DIRECTORY DOMAIN SERVICE UNTUK MANAJEMEN HAK AKSES PENGGUNA DI SERVER SMK AL-BADAR

Moch Afdal Dzikri Maulana[1*], Arip Solehudin[2], Carudin[3]

[1,2,3]Universitas Singaperbangsa Karawan; Jl.HS.Ronggo Waluyo, Paseurjaya, Telukjambe Timur, Karawang, Jawa Barat 41361;Telp. (0267) 641177

Keywords:
Active Directory Domain Services, Role-Based Access Control, Manajemen Hak Akses*, Windows Server 2022,* Jaringan Sekolah.

Corespondent Email:
2210631170132@student.unsika.ac.id

Abstrak. Pengelolaan hak akses pengguna yang belum terstruktur dapat menyebabkan tumpang tindih akses, serta menyulitkan administrasi jaringan. Permasalahan tersebut terjadi di SMK Al-Badar, di mana pengelolaan akun pengguna masih dilakukan secara manual dan belum berbasis peran. Penelitian ini bertujuan mengimplementasikan *Role-Based Access Control* (RBAC) pada *Active Directory Domain Services* (AD DS) untuk meningkatkan manajemen hak akses pengguna di Server SMK Al-Badar. Metode yang digunakan adalah *Network Development Life Cycle* (NDLC) yang meliputi tahapan analisis, perancangan, simulasi, implementasi, monitoring, dan manajemen. Implementasi dilakukan menggunakan *Windows Server* 2022 dengan pembentukan domain, organizational unit, grup keamanan, akun pengguna, serta konfigurasi *Group Policy* sesuai peran pengguna, yaitu administrator, staf tata usaha, guru, dan siswa. Pengujian dilakukan melalui skenario akses folder dan perhitungan violation rate. Hasil penelitian menunjukkan bahwa penerapan RBAC pada AD DS mampu meningkatkan efisiensi pengelolaan akun, memperjelas pembagian hak akses, serta meminimalkan akses tidak sah terhadap sumber daya jaringan.

Abstract. *Unstructured user access rights management can lead to overlapping access and complicate network administration. This issue occurs at SMK Al-Badar, where user account management is still handled manually and is not role-based. This study aims to implement Role-Based Access Control (RBAC) on Active Directory Domain Services (AD DS) to improve user access rights management on the SMK Al-Badar server. The method employed is the Network Development Life Cycle (NDLC), which includes the stages of analysis, design, simulation, implementation, monitoring, and management. The implementation uses Windows Server 2022 by establishing a domain, organizational units, security groups, user accounts, and configuring Group Policy according to user roles, namely administrators, administrative staff, teachers, and students. System testing is conducted through folder access scenarios and violation rate calculations. The results indicate that implementing RBAC on AD DS enhances the efficiency of user account management, clarifies role-based access allocation, and minimizes unauthorized access to network resources.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan jaringan komputer terus mengalami kemajuan yang signifikan, sehingga mendorong institusi pendidikan untuk mengadopsi sistem pengelolaan jaringan yang terpusat, aman, dan efisien. Di lingkungan Sekolah Menengah Kejuruan (SMK), pemanfaatan jaringan komputer tidak hanya mendukung proses pembelajaran berbasis teknologi informasi, tetapi juga digunakan dalam pengelolaan data akademik, administrasi sekolah, serta akses terhadap berbagai sumber daya sistem oleh beragam jenis pengguna. Kondisi tersebut menuntut adanya mekanisme pengelolaan hak akses yang terstruktur agar setiap pengguna memperoleh akses sesuai dengan peran dan tanggung jawabnya.

Active Directory Domain Services (AD DS) merupakan layanan direktori yang banyak digunakan dalam pengelolaan identitas, autentikasi, dan otorisasi pengguna pada jaringan berbasis sistem operasi *Windows*. AD DS memungkinkan *administrator* jaringan untuk mengelola akun pengguna, perangkat, serta kebijakan keamanan secara terpusat, sehingga meningkatkan konsistensi dan efisiensi manajemen jaringan [1]. Namun, dalam praktiknya di lingkungan sekolah, pengelolaan hak akses pada AD DS sering kali masih dilakukan secara umum tanpa pembagian peran yang jelas. Kondisi ini berpotensi menimbulkan berbagai permasalahan, seperti pemberian hak akses berlebihan (*over-privileged access*), kesulitan administrasi, serta meningkatnya risiko keamanan sistem [2].

Role-Based Access Control (RBAC) merupakan model pengendalian akses yang memberikan hak akses kepada pengguna berdasarkan peran tertentu dalam suatu organisasi. Pendekatan ini terbukti mampu menyederhanakan proses administrasi hak akses, meningkatkan keamanan sistem, serta mengurangi kesalahan konfigurasi [3]. Sejumlah penelitian terdahulu menunjukkan bahwa penerapan AD DS efektif dalam manajemen jaringan, sementara RBAC mampu meningkatkan kontrol akses dan keamanan sistem. Akan tetapi, sebagian besar penelitian tersebut masih berfokus pada lingkungan perusahaan atau organisasi berskala besar dan belum banyak membahas penerapan RBAC yang terintegrasi dengan AD DS secara kontekstual di lingkungan pendidikan menengah.

Lingkungan SMK memiliki karakteristik operasional yang khas dengan keberagaman peran pengguna, seperti *administrator*, guru, siswa, dan staf tata usaha, yang masing-masing memiliki kebutuhan serta tingkat akses yang berbeda. Tanpa pengelolaan hak akses yang terstruktur, kondisi ini dapat menurunkan efisiensi pengelolaan sistem serta meningkatkan potensi pelanggaran keamanan. Pengelolaan hak akses pengguna yang tidak terstruktur pada lingkungan pendidikan, khususnya di *laboratorium* komputer sekolah, dapat meningkatkan risiko pelanggaran keamanan data serta penyalahgunaan akses terhadap sumber daya sistem. Oleh karena itu, diperlukan penerapan sistem direktori terpusat yang mampu mengatur dan membatasi hak akses pengguna secara sistematis sesuai dengan peran dan tanggung jawabnya [14].

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk merancang dan mengimplementasikan *Role-Based Access* Control pada *Active Directory Domain Services* guna meningkatkan manajemen hak akses pengguna di server SMK Al-Badar. Kebaruan penelitian ini terletak pada penerapan RBAC yang disesuaikan dengan struktur organisasi dan kebutuhan operasional nyata di lingkungan SMK, sehingga diharapkan dapat memberikan kontribusi praktis berupa model implementasi pengelolaan hak akses yang lebih aman, efisien, dan mudah dikelola sebagai referensi bagi institusi pendidikan sejenis.

2. TINJAUAN PUSTAKA

2.1 Active Directory Domain Services

Active Directory Domain Services (AD DS) merupakan layanan direktori pada sistem operasi *Windows Server* yang digunakan untuk mengelola identitas pengguna, perangkat, serta kebijakan keamanan jaringan secara terpusat. AD DS menyediakan mekanisme autentikasi dan otorisasi yang memungkinkan administrator mengatur akun pengguna dan hak akses terhadap sumber daya jaringan melalui struktur *domain*, *organizational unit* (OU), dan grup keamanan [1].

Penerapan AD DS terbukti mampu meningkatkan efisiensi pengelolaan jaringan dan konsistensi kebijakan keamanan,

khususnya pada lingkungan institusi pendidikan dan organisasi yang memiliki banyak pengguna [2]. Selain itu, sentralisasi autentikasi pengguna menggunakan *Active Directory Domain Services* memungkinkan pengelolaan sumber daya jaringan dilakukan secara lebih efisien serta menjamin konsistensi penerapan kebijakan keamanan pada seluruh perangkat yang terhubung dalam domain [11].

Integrasi AD DS dengan layanan pendukung seperti file *server* dan *Domain Name System* (DNS) memungkinkan pengelolaan akses data dilakukan secara terkontrol dan terstruktur [5], [8]. Dalam penelitian ini, AD DS digunakan sebagai platform utama untuk implementasi manajemen hak akses pengguna berbasis peran.

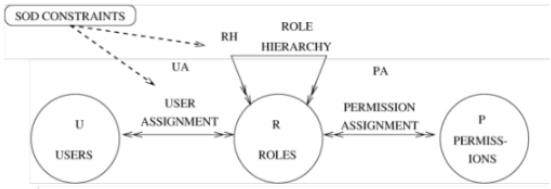
2.2 *Role-Based Access Control*

Role-Based Access Control (RBAC) merupakan model pengendalian akses yang memberikan hak akses kepada pengguna berdasarkan peran (*role*) yang dimilikinya dalam suatu organisasi. Setiap peran merepresentasikan sekumpulan hak akses yang disesuaikan dengan fungsi dan tanggung jawab pengguna. Pendekatan RBAC bertujuan untuk menyederhanakan administrasi hak akses, meningkatkan keamanan sistem, serta meminimalkan risiko kesalahan pemberian akses [3].

Penerapan RBAC pada sistem berbasis *Active Directory* dapat dilakukan melalui pemanfaatan grup keamanan (*security group*) dan penerapan kebijakan *Group Policy Object* (GPO). Penelitian Sadikin dan Sari menunjukkan bahwa penerapan kebijakan keamanan berbasis GPO pada *Active Directory Domain Services* mampu meningkatkan pengendalian akses pengguna dan memperkuat keamanan jaringan secara signifikan [7].

Selain itu, implementasi RBAC terbukti efektif dalam mencegah pemberian hak akses berlebihan (*over-privileged access*) dan meningkatkan keandalan sistem informasi. Penelitian Nasich dkk. menyatakan bahwa RBAC mampu meningkatkan kontrol akses serta mengurangi potensi penyalahgunaan hak akses pada sistem informasi berbasis peran [9]. Studi lain juga menegaskan bahwa RBAC sangat sesuai diterapkan pada lingkungan akademik karena mampu mengakomodasi berbagai peran pengguna dengan kebutuhan akses yang berbeda, seperti administrator, staf, guru, dan siswa [12].

Berdasarkan penelitian terdahulu tersebut, model RBAC digunakan dalam penelitian ini sebagai dasar perancangan pembagian hak akses pengguna pada sistem jaringan sekolah. Berikut ditampilkan Gambar 1 yang menggambarkan model *Role-Based Access Control*.



Gambar 1. Model *Role-base access control*

2.3 *Network Development Life Cycle*

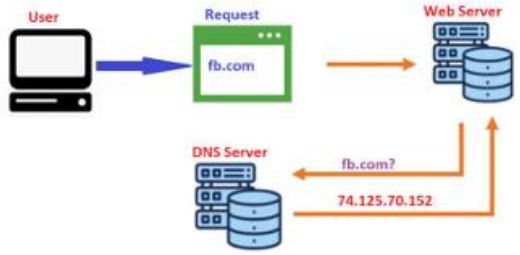
Network Development Life Cycle (NDLC) merupakan metode pengembangan jaringan komputer yang terdiri dari tahapan analisis, perancangan, implementasi, pengujian, monitoring, dan manajemen. Metode ini digunakan untuk memastikan bahwa sistem jaringan yang dibangun sesuai dengan kebutuhan pengguna dan mampu beroperasi secara optimal [15].

Penggunaan NDLC dalam penelitian jaringan komputer dinilai efektif karena memberikan tahapan kerja yang sistematis dan mudah direplikasi. Penelitian oleh Naim dkk. menunjukkan bahwa NDLC mampu membantu proses analisis dan pengembangan jaringan secara terstruktur serta meningkatkan kualitas kinerja jaringan [13]. Oleh karena itu, metode NDLC digunakan sebagai kerangka kerja dalam penelitian ini untuk merancang dan mengimplementasikan sistem AD DS berbasis RBAC.

2.3 *Domain Name System*

*Domain Name Syste*m (DNS) merupakan sistem penamaan terdistribusi yang berfungsi untuk menerjemahkan nama domain menjadi alamat IP. Dalam lingkungan *Active Directory*, DNS memiliki peran yang sangat penting karena digunakan dalam proses pencarian *domain controller*, autentikasi pengguna, serta komunikasi antar perangkat jaringan. Tanpa konfigurasi DNS yang tepat, layanan AD DS tidak dapat berjalan dengan baik. Oleh karena itu, DNS menjadi komponen pendukung utama

dalam implementasi *Active Directory Domain Services* [5]. Berikut gambar 2 Cara Kerja DNS



Gambar 2. Cara Kerja DNS

2.4 *Violation Rate*

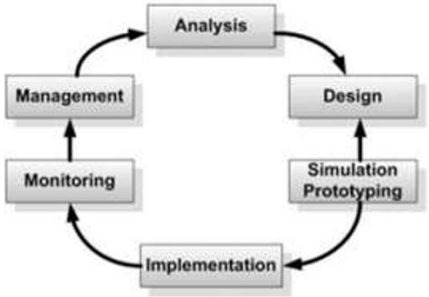
Violation rate merupakan parameter yang digunakan untuk mengukur tingkat pelanggaran akses pengguna terhadap kebijakan hak akses yang telah ditetapkan. Pelanggaran akses dapat berupa upaya pengguna mengakses sumber daya yang tidak sesuai dengan perannya. Pengukuran violation rate digunakan untuk mengevaluasi efektivitas sistem pengendalian akses yang diterapkan [6]. Secara umum, perhitungan violation rate dirumuskan sebagai berikut [6]:

$$\text{Violation Rate} = \frac{\textbf{Jumlah Pelanggaran}}{\textbf{Jumlah Skenario Pengujian}} \text{ x } 100\ \%$$

Semakin kecil nilai violation rate, maka semakin baik tingkat kepatuhan pengguna terhadap kebijakan hak akses. Dalam penelitian ini, violation rate digunakan sebagai indikator untuk menilai efektivitas penerapan RBAC pada *Active Directory Domain Services*.

3. METODE PENELITIAN

Penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC) sebagai kerangka kerja untuk merancang, mengimplementasikan, dan mengevaluasi sistem manajemen hak akses pengguna berbasis *Role-Based Access Control* (RBAC) pada layanan *Active Directory Domain Services* (AD DS). Metode NDLC dipilih karena menyediakan tahapan pengembangan jaringan yang sistematis dan terstruktur, sehingga memungkinkan penelitian ini dapat direplikasi oleh peneliti lain pada lingkungan jaringan yang serupa. Gambar 3 Menunjukan gambar model NDLC :

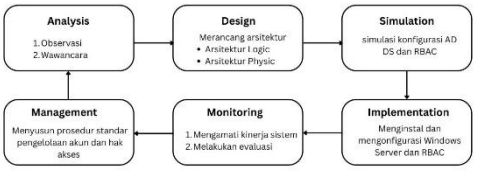


Gambar 3. *Network Development Life Cycle* (NDLC)

3.1 Rancangan Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah *Network Development Life Cycle* (NDLC). NDLC merupakan metode pengembangan jaringan yang terdiri dari tahapan terstruktur mulai dari analisis kebutuhan hingga pengelolaan jaringan secara berkelanjutan. Metode ini dipilih karena sesuai untuk perancangan dan implementasi sistem jaringan terpusat yang membutuhkan perencanaan matang, pengujian, serta evaluasi performa jaringan [1].

NDLC telah banyak digunakan dalam penelitian jaringan komputer karena mampu menghasilkan sistem yang terdokumentasi dengan baik dan mudah direplikasi pada lingkungan jaringan lain dengan karakteristik serupa [2]. Tahapan NDLC yang digunakan pada penelitian ini meliputi: analisis, desain, implementasi, pengujian, dan manajemen. Berikut gambar 4. Alur penelitian NDLC:



Gambar 4. Alur penelitian NDLC

3.2 Tahap Analisis

Tahap analisis dilakukan untuk mengidentifikasi kondisi jaringan yang berjalan di lingkungan laboratorium komputer. Analisis meliputi struktur jaringan eksisting, mekanisme autentikasi pengguna, pengelolaan akun, serta pengaturan hak akses terhadap sumber daya jaringan. Hasil analisis menunjukkan bahwa pengelolaan pengguna masih bersifat manual dan belum menerapkan pembatasan akses berdasarkan peran, sehingga berpotensi menimbulkan pelanggaran kebijakan akses (*access violation*) [3].

Selain itu, dilakukan analisis kebutuhan sistem untuk menentukan peran pengguna (*role*), seperti administrator, guru, dan siswa, serta layanan jaringan yang dapat diakses oleh masing-masing peran. Analisis ini menjadi dasar dalam perancangan RBAC pada *Active Directory Domain Services*.

3.3 Tahap Desain

Tahap desain meliputi perancangan topologi jaringan fisik dan logis, struktur Active Directory, pembagian *Organizational Unit* (OU), serta perancangan kebijakan akses berbasis peran. Pada tahap ini juga dirancang arsitektur DNS sebagai layanan pendukung AD DS, karena DNS berperan penting dalam proses resolusi nama dan autentikasi domain [4].

3.3.1 Topologi logic

Desain arsitektur logik menggambarkan rancangan konseptual sistem tanpa memperhatikan detail perangkat keras yang digunakan. Fokus utamanya adalah bagaimana sistem RBAC pada AD DS bekerja secara konseptual dalam mengatur hubungan antar entitas pengguna dan kebijakan akses.

3.3.2 Topologi Fisik

Desain arsitektur fisik menjelaskan penerapan nyata dari desain logik ke dalam bentuk infrastruktur jaringan dan perangkat keras. Pada tahap ini, rancangan difokuskan pada penentuan spesifikasi perangkat, konfigurasi *Server*, serta topologi jaringan yang digunakan di SMK Al-Badar Cipulus.

3.4 Tahap Simulasi

Pada tahap ini dilakukan simulasi dan pembuatan prototipe sistem *Active Directory Domain* ***Services*** **(**AD DS**)** dengan penerapan *Role-Based Access Control* **(**RBAC**)** dalam lingkungan virtual atau terbatas. Simulasi bertujuan untuk menguji rancangan sistem sebelum diterapkan pada *Server* utama di SMK Al-Badar. Proses ini mencakup instalasi *Windows Server* dan konfigurasi awal AD DS pada *Server* uji, pembuatan *Domain* sekolah, serta penentuan *Role* pengguna seperti siswa, guru, *staf* tata usaha, dan *administrator*. Selain itu, dilakukan pengujian awal terhadap akun yang dibuat serta penerapan kebijakan hak akses berdasarkan *Role* untuk memastikan rancangan sesuai dengan kebutuhan dan tidak menimbulkan konflik akses antar pengguna.

3.5 Tahap Implementasi

Tahap implementasi dilakukan di lingkungan nyata, yaitu jaringan SMK Al-Badar Cipulus. Server sekolah diinstal dengan *Windows Server* dan dikonfigurasi sebagai *Domain Controller* yang menjalankan layanan Active Directory Domain Services (AD DS). Selanjutnya dilakukan konfigurasi Domain sekolah, pembentukan struktur role pengguna yang meliputi siswa, guru, staf tata usaha, dan administrator, serta penerapan *Role-Based Access Control* (RBAC) melalui kebijakan *Group Policy* yang disesuaikan dengan kebutuhan masing-masing peran.

Proses implementasi juga mencakup integrasi akun pengguna dan komputer klien ke dalam Domain sekolah untuk memastikan proses autentikasi dan otorisasi dapat berjalan secara terpusat dan konsisten. Integrasi komputer klien ke dalam Domain dilakukan guna menjamin bahwa seluruh proses login pengguna serta akses terhadap sumber daya jaringan dapat diverifikasi secara aman melalui mekanisme *Active Directory*, sebagaimana diterapkan pada penelitian sebelumnya yang mengombinasikan *Active Directory* dengan sistem autentikasi jaringan terpusat [10].

Mekanisme autentikasi terpusat tersebut memungkinkan pengelolaan hak akses dilakukan secara lebih terkontrol dan meminimalkan potensi kesalahan konfigurasi pada sisi klien. Tahap implementasi ini kemudian dibandingkan dengan kondisi jaringan sebelum penerapan *Active Directory Domain Services* berbasis RBAC untuk menilai peningkatan efisiensi manajemen akun pengguna serta efektivitas pengendalian hak akses di lingkungan sekolah.

3.6 Tahap Monitoring

Tahap monitoring dilakukan untuk memastikan bahwa sistem *Active Directory Domain Services* (AD DS) dengan penerapan *Role-Based Access Control* (RBAC) yang telah diimplementasikan dapat berjalan sesuai dengan rancangan serta memenuhi tujuan pengamanan hak akses pengguna. Kegiatan monitoring meliputi pengamatan langsung terhadap proses autentikasi pengguna dan pengujian akses terhadap sumber daya jaringan, khususnya folder bersama, berdasarkan peran masing-masing pengguna. Evaluasi sistem dilakukan secara teknis dengan mengamati apakah setiap pengguna hanya dapat mengakses sumber daya yang sesuai dengan hak akses yang telah ditetapkan. Untuk mengukur tingkat efektivitas penerapan RBAC, penelitian ini menggunakan metode perhitungan *violation rate*, yaitu dengan membandingkan jumlah pelanggaran akses yang terjadi terhadap total skenario pengujian yang dilakukan. Nilai violation rate yang dihasilkan digunakan sebagai indikator keberhasilan sistem dalam mencegah akses yang tidak sah, di mana semakin kecil nilai violation rate menunjukkan semakin baik tingkat pengendalian akses yang diterapkan pada sistem AD DS.

3.7 Tahap Management

Tahap ini merupakan bagian dari pengelolaan berkelanjutan terhadap sistem yang telah dibangun di SMK Al-Badar Cipulus. Fokus utamanya adalah menjaga keamanan sistem melalui penerapan kebijakan akses berbasis *Role-Based Access Control* (RBAC) **pada** *Active Directory Domain Services* (AD DS**)**, melakukan pemeliharaan akun pengguna sesuai dinamika peran di sekolah (siswa baru, guru, *staf*, maupun perubahan *Role*), serta memperbarui kebijakan hak akses apabila terjadi penyesuaian kebutuhan. Selain itu, diberikan pelatihan dasar kepada *staf* sekolah, khususnya *administrator* jaringan, terkait penggunaan dan pengelolaan AD DS berbasis RBAC. Evaluasi sistem juga dilakukan secara berkala untuk memastikan sistem berjalan optimal, efisien, dan tetap sesuai dengan kebutuhan pengelolaan TI di lingkungan sekolah

4. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan *implementasi Role-Based Access Control* (RBAC) pada *Active Directory Domain Services* (AD DS) yang diterapkan di *Server* SMK Al-Badar. Hasil ini menjelaskan penerapan RBAC dan AD DS sebelum serta sesudah proses pengujian dilakukan, yang mengikuti tahapan Analisis, Desain, Simulasi, Implementasi, Monitoring, dan Manajemen sebagaimana telah direncanakan sebelumnya. Fokus penelitian terletak pada penerapan sistem manajemen hak akses pengguna berdasarkan peran (*Role*) menggunakan AD DS, yang meliputi pengelolaan akun siswa, guru, staf tata usaha, dan administrator secara terpusat.

Dalam bab ini juga disajikan penjelasan dan pembahasan terhadap setiap tahapan proses tersebut sesuai dengan metodologi NDLC yang digunakan, mulai dari analisis kebutuhan jaringan, perancangan arsitektur sistem, simulasi lingkungan uji, implementasi *Server Domain*, hingga pemantauan dan pengelolaan sistem yang telah berjalan. Bab ini menggambarkan bagaimana penerapan RBAC pada AD DS dapat meningkatkan efisiensi administrasi jaringan, memperkuat keamanan data, serta menciptakan struktur manajemen pengguna yang lebih sistematis dan profesional di lingkungan SMK Al-Badar.

memainkan peran penting dalam sebuah artikel ilmiah. Bagian ini menjawab permasalahan, menginterpretasikan hasil penelitian dan temuan menjadi pengetahuan yang telah diketahui, menegaskan dan/atau kontras dengan penelitian-peneliti lain, mengkonstruksi teori baru, dan/atau memodifikasi teori sebelumnya. Pembahasan juga harus memuat implikasi hasil teoritis dan implementasi.

4.1 Analisis

Tahap analisis dilakukan untuk memahami kondisi aktual jaringan komputer di SMK Al-Badar serta mengidentifikasi kebutuhan sistem yang diperlukan dalam penerapan *Role-Based Access Control* (RBAC) pada *Active Directory Domain Services* (AD DS). Analisis ini melibatkan dua kegiatan utama, yaitu observasi langsung terhadap infrastruktur jaringan sekolah dan wawancara dengan pihak-pihak yang terkait dengan pengelolaan jaringan.

4.2 Observasi

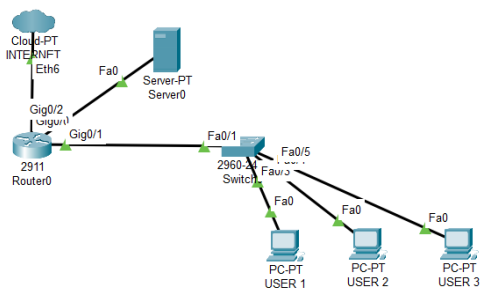
Pada tahap observasi, peneliti melakukan pengamatan langsung terhadap kondisi jaringan komputer dan sistem manajemen pengguna di lingkungan SMK Al-Badar. Berdasarkan hasil pengamatan, ditemukan bahwa pengelolaan akun pengguna masih dilakukan secara manual tanpa adanya sistem autentikasi terpusat. Setiap komputer berdiri sendiri tanpa koneksi ke *Server* pusat, sehingga administrator jaringan harus melakukan konfigurasi satu per satu pada tiap perangkat.

Selain itu, belum terdapat pembagian peran pengguna yang jelas antara siswa, guru, *staf* tata usaha, dan *administrator*. Akibatnya, sering terjadi tumpang tindih akses terhadap folder maupun aplikasi yang seharusnya dibatasi sesuai peran pengguna. Peneliti juga menemukan bahwa belum diterapkan kebijakan keamanan jaringan secara terpusat menggunakan *Group Policy*, sehingga pengawasan dan perlindungan data menjadi kurang optimal.

4.2.1 Analisis Jaringan

Analisis jaringan dilakukan untuk mengetahui kondisi serta *topologi* jaringan yang sudah ada di SMK Al-Badar sebelum penerapan sistem baru berbasis *Active Directory Domain Services* (AD DS) dengan mekanisme *Role-Based Access Control* (RBAC). Tahap ini bertujuan untuk memahami struktur koneksi antarperangkat, distribusi *Server*, serta pola komunikasi data di lingkungan sekolah.

Berikut gambar 5 *topologi* sekolah :



Gambar 5. *Topologi* Sekolah

4.2.2 Analisis Kebutuhan Perangkat Keras

Berikut merupakan Spesipikasi perangkat keras yang digunakan dalam penelitian ini dan digunakan untuk menjalankan sistem *Active Directory Domain Services* (ADDS) dengan mekanisme *Role-Based Access Control* (RBAC) dapat dilihat dalam tabel 1 berikut:

Tabel 1. Kebutuhan perangkat keras

NO	Perangkat Keras	Spesifikasi
1	*Server Domain ContRoler*	CPU 8-core
2	*Router*	Router Gigabit dengan NAT
3	*Switch*	Tp-link TL-SG1005D
4	*Processor*	Intel i5-1135G7
5	Harddisk	SSD 500GB

4.2.3 Analisis Kebutuhan Perangkat Lunak

Berikut merupakan Spesifikasi perangkat lunak yang digunakan dalam penelitian ini dan digunakan juga untuk menjalankan sistem *Active Directory Domain Services* (ADDS) dengan mekanisme *Role-Based Access Control* (RBAC) dapat dilihat dalam tabel 2 berikut:

Tabel 2 kebutuhan perangkat lunak

NO	Perangkat Keras	Spesifikasi
1	*Windows Server*	*Windows Server* 2022
2	Aplikasi Simulasi Sistem	*Virtual-Box*
3	Sistem Operasi	Windows 11

4.3 Wawancara

Kegiatan wawancara dilakukan dengan *administrator* jaringan untuk memperoleh informasi lebih detail mengenai permasalahan dan kebutuhan sistem. Dari hasil wawancara diketahui bahwa pihak sekolah mengalami kesulitan dalam mengelola banyaknya akun pengguna serta membatasi hak akses masing-masing pengguna.

Administrator jaringan menyampaikan bahwa sering terjadi kesalahan akses, seperti siswa yang dapat membuka folder milik guru atau staf, karena tidak adanya sistem pembagian hak akses berbasis peran. Selain itu, proses pemeliharaan jaringan menjadi lambat karena pengaturan dilakukan secara manual di setiap

komputer. Berdasarkan hasil wawancara ini, pihak sekolah berharap adanya sistem terpusat yang dapat mengelola akun pengguna secara otomatis, mengatur hak akses sesuai peran, dan meningkatkan keamanan jaringan sekolah melalui penerapan AD DS dengan metode RBAC.

4.4 Desain

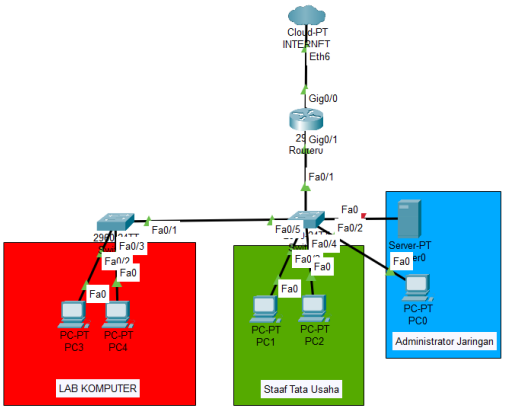
Pada tahap desain, dilakukan perancangan menyeluruh terhadap sistem jaringan untuk mendukung implementasi *Role-Based Access Control* (RBAC) pada *Active Directory Domain Services* (AD DS) di lingkungan SMK Al-Badar. Pertama, dirancang topologi fisik jaringan untuk memastikan konektivitas antarperangkat seperti *Server Domain controller*, *switch*, *router*, dan komputer klien. Kedua, dirancang topologi logic untuk memastikan konektivitas sesuai dengan kebutuhan, termasuk pengaturan subnetting, dan routing.

Selain itu, pada tahap desain juga dirancang **alur konfigurasi** *Active Directory Domain Services* (AD DS) berbasis *Role-Based Access Control* (RBAC) yang disesuaikan dengan kebutuhan jaringan di SMK Al-Badar. Perancangan ini mencakup pembuatan *Organizational Unit* (OU) untuk setiap kategori pengguna seperti siswa, guru, staf tata usaha, dan *administrator*, serta penerapan ***Group Policy Object*** (GPO) yang mengatur hak akses dan pembatasan sesuai peran masing-masing.

Dengan desain yang terencana dan disesuaikan dengan kebutuhan operasional sekolah, sistem AD DS **berbasis** RBAC diharapkan mampu meningkatkan efisiensi manajemen akun pengguna, memperkuat keamanan data, serta mempermudah pengawasan jaringan secara terpusat. Desain yang baik ini menjadi landasan penting agar implementasi sistem dapat berjalan optimal dan memberikan manfaat yang signifikan bagi seluruh civitas akademika di SMK Al-Badar.

4.4.1 Topologi fisik

Disajikan ilustrasi *topologi* fisik yang menggambarkan hubungan antarperangkat, alur konektivitas, serta pembagian segmen jaringan sesuai fungsi masing-masing. SBerikut adalah gambar 6 Topologi Fisik :



Gambar 6. *Topologi* Fisik

Topologi ini menyediakan satu komputer administrator untuk kebutuhan konfigurasi, pemantauan, dan perawatan jaringan, khususnya dalam pengelolaan *Active Directory Domain Services* (AD DS). Perangkat staf tata usaha dan komputer laboratorium terhubung melalui switch sehingga seluruh pengaturan hak akses berbasis peran *Role-Based Access Control* (RBAC) dapat diterapkan secara terpusat tanpa konfigurasi manual pada masing-masing perangkat. Dengan struktur fisik tersebut, ketersediaan jaringan dapat terjaga dan pengelolaan jaringan di SMK Al-Badar menjadi lebih efisien, aman, dan sesuai kebutuhan operasional sekolah.

4.4.1 Topologi fisik

Untuk menggambarkan pembagian alamat IP serta struktur logis jaringan yang digunakan dalam implementasi sistem, disusun tabel *topologi* logik yang memuat informasi perangkat, segmentasi jaringan, dan pengalokasian alamat sesuai fungsinya. Berikut adalah tabel 3 *Topologi* Logic :

Tabel 3 *Topologi Logic*

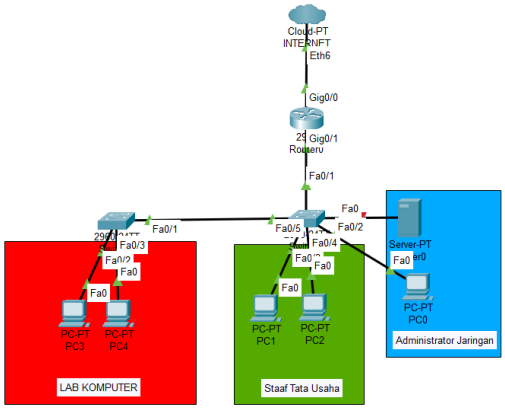
NO	Nama	Keterangan
1	Router	192.168.0.1/24
2	*Server*	192.168.1.1/24
3	DNS	192.168.1.1
4	Administrator	192.168.10.1/24
5	PC – *Staff* TU	192.168.10.2 s/d 192.168.10.10/24 (DHCP)

6	PC Lab Komputer	192.168.20.2 s/d 192.168.20.40/24 (DHCP)

Tabel *topologi* logik pada tahap desain menunjukkan bahwa setiap perangkat yang terhubung ke jaringan diberikan alamat IP yang berbeda untuk memastikan komunikasi dapat berlangsung tanpa benturan. *Server* menggunakan alamat IP statis sebagai pusat layanan *Domain*, sedangkan *router* berfungsi sebagai *gateway* utama bagi seluruh perangkat yang berada dalam jaringan lokal.

4.5 Simulasi

Pada tahap simulasi dengan menggunakan *sofware* untuk simulasi jaringan yaitu *cisco packet treacer*, berikut gambar 4.3 Simulasi *Topologi*:



Gambar 7. Simulasi *Topologi*

Tahap simulasi ini dibuat bedasarkan topologi fisik dan juga topologi logic dari tahap desain. Hasil yang didapatkan pada simulasi ini semua perangkat dapat terhubung dengan baik, berikut tabel 4 Tabel Simulasi:

Tabel 3 *Topologi Logic*

NO	Perangkat	Keterangan
1	Cloud-PT INTERNET	Menggambarkan akses internet
2	2301 Router0	Media jaringan yang berfungsi mengatur bandwidth serta lalu lintas data dalam jaringan.
3	2960-24TT Switch0	Media jaringan yang berfungsi membagi jaringan kepada perangkat *User* menggunakan kabel
4	Server-PT Server0	Perangkat yang menyediakan berbagai layanan jaringan bagi perangkat lain dalam jaringan.
5	PC-PT PC0	Perangkat *User* yang menggunakan kabel untuk terkoneksi dengan media jaringan
6		Menjelaskan bahwa perangkat sudah terkoneksi dengan perangkat lain melalui kabel straight

4.6 Implementasi

Pada tahap ini implementasi merupakan proses penerapan rancangan sistem *Active Directory Domain Services* (AD DS) dengan mekanisme *Role-Based Access Control* (RBAC) pada lingkungan jaringan SMK Al-Badar. Implementasi dilakukan berdasarkan hasil analisis dan desain yang telah disusun sebelumnya, sehingga sistem dapat berfungsi sesuai kebutuhan manajemen hak akses pengguna di sekolah. Tahapan implementasi ini meliputi persiapan *Server*, instalasi layanan AD DS, pembuatan *Domain*, pembentukan struktur *Organizational Unit* (OU), konfigurasi peran pengguna, penerapan *Group Policy*, integrasi komputer *client*, serta pengujian hak akses berdasarkan *Role*.

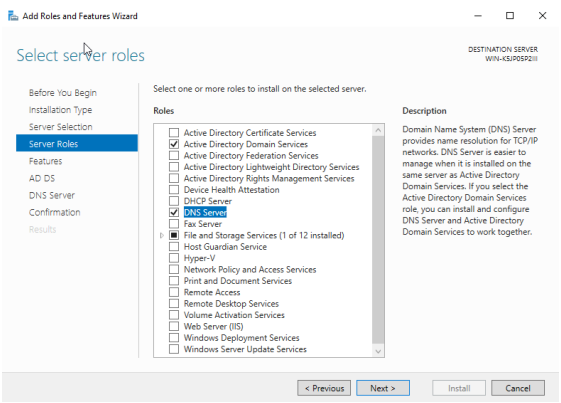
4.6.1 Persiapan Server

Tahap awal dilakukan dengan menyiapkan perangkat *Server* yang akan digunakan sebagai pusat pengelolaan *Domain*. Kegiatan yang dilakukan meliputi pemasangan sistem operasi *Windows Server* 2022, konfigurasi identitas perangkat, serta penetapan

alamat IP statis agar *Server* dapat berkomunikasi secara stabil dengan seluruh perangkat dalam jaringan.

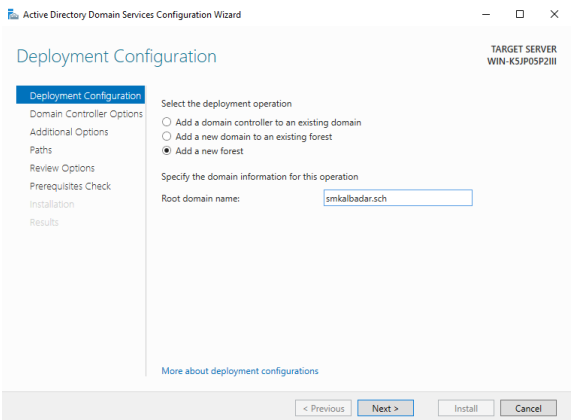
4.6.2 *Instalasi Active Directory Domain Service*

Setelah *Server* siap digunakan, langkah berikutnya yaitu melakukan instalasi layanan Active Directory *Domain* Services melalui *Server* Manager. Proses ini dilakukan dengan menambahkan peran (*Role*) AD DS, kemudian melanjutkan instalasi hingga *Server* siap dipromosikan menjadi *Domain* Controller. Pada tahapan ini belum terjadi pembentukan *Domain*, melainkan hanya persiapan layanan direktori yang diperlukan untuk proses selanjutnya. Berikut Gambar *Instalasi Active Directory Domain Services*



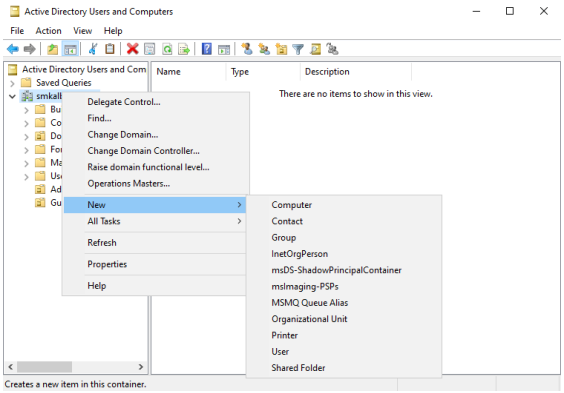
4.6.3 Pembuatan Server Sekolah

Setelah *Active Directory Domain Services* (AD DS) terpasang, *Server* dipromosikan menjadi *Domain Controller* dengan membentuk *Domain* baru bagi lingkungan jaringan SMK Al-Badar. Nama *Domain* yang digunakan adalah smkalbadar.sch sesuai dengan identitas institusi. Pada tahap ini ditetapkan pula mode fungsional *Domain*, konfigurasi DNS internal, serta pengaturan *Directory Services Restore Mode* (DSRM) untuk kebutuhan pemeliharaan.



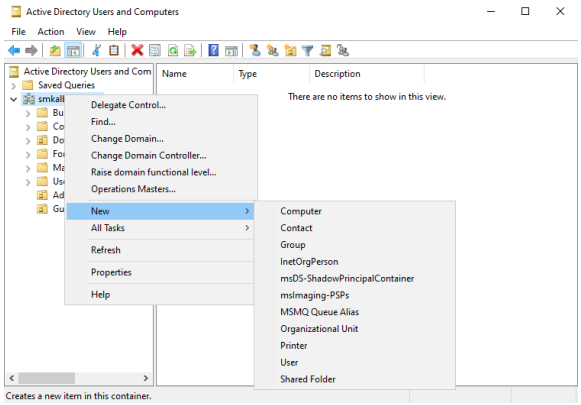
4.6.4 Pembentukan Struktur Organizational Unit (OU)

Tahap berikutnya adalah penyusunan struktur *Organizational Unit* (OU) yang menjadi wadah pengelompokan objek pengguna sesuai peran masing-masing.



4.6.5 Pembuatan *Role* dan Grup Keamanan

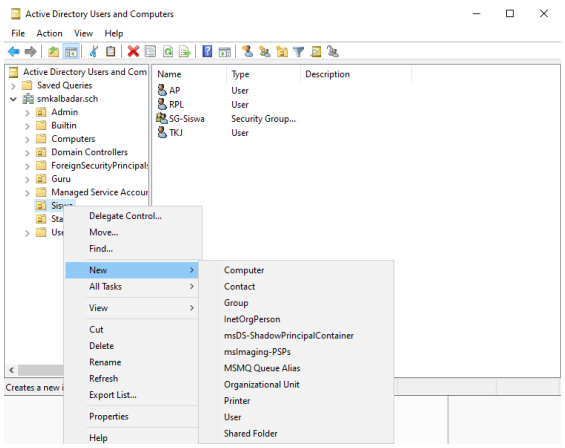
Setelah *Organizational Unit* (OU) terbentuk, dilakukan pembuatan *Role* pengguna melalui pembentukan kelompok keamanan (*security group*). Masing-masing *Role* diberikan kelompok tersendiri. Berikut gambar Pembuatan *Role* dan *Group*:



4.6.6 Pembuatan Akun Pengguna

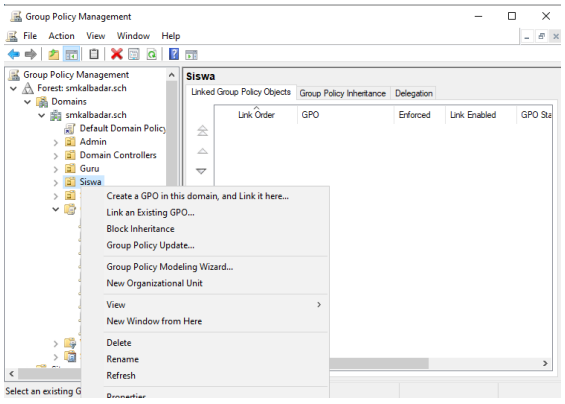
Akun pengguna dibuat berdasarkan data pengguna SMK Al-Badar yang terdiri dari *administrator*, guru, siswa, dan *staf* tata usaha. Setiap akun dibuat dengan format penamaan

yang konsisten serta diberi kata sandi awal sesuai standar keamanan, Akun dibuat dialam *Organizational Unit* (OU) masing-masing dan dimasukkan ke dalam grup keamanan sesuai perannya sehingga setiap pengguna akan memperoleh hak akses berdasarkan *Role* yang diberikan. Berikut gambar Pembuatan Akun Pengguna:



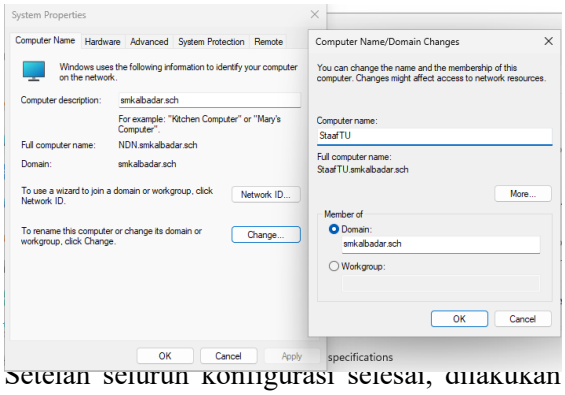
4.6.7 Konfigurasi *Goup Policy* (GPO)

Penerapan *Group Policy* dilakukan untuk mengatur batasan akses folder, Kebijakan diterapkan menggunakan *Group Policy Management Console* dan ditautkan langsung dengan *Organizational Unit* (OU) yang bersangkutan. Berikut gambar Konfigurasi *Group Policy*:

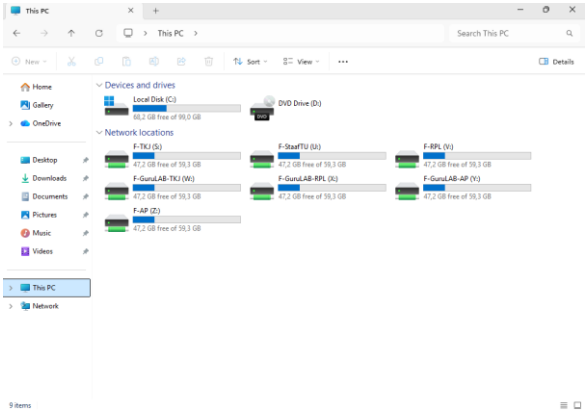


4.6.8 Integrasi Komputer Client ke Domain

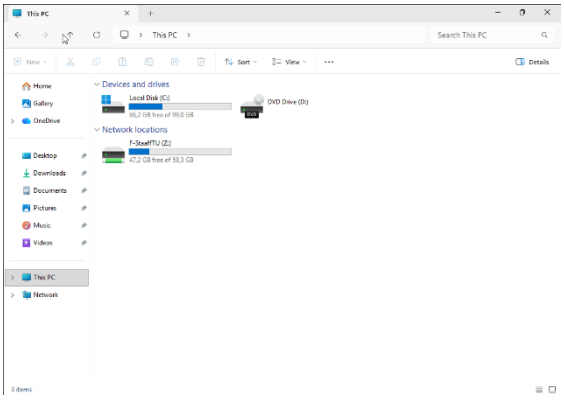
Komputer yang digunakan oleh guru, siswa, dan staf tata usaha kemudian diintegrasikan ke dalam *Domain* smkalbadar.sch, Proses ini dilakukan dengan menghubungkan perangkat ke jaringan *Server*, kemudian melakukan *Domain* join melalui pengaturan sistem. Berikut gambar Integrasi Komputer *Client* ke *Domain*:



Setelah seluruh konfigurasi selesai, dilakukan pengujian untuk memastikan bahwa setiap pengguna memperoleh hak akses sesuai peran yang telah ditentukan. Pengujian dilakukan dengan login menggunakan akun dari masing-masing kategori pengguna. Berikut gambar Pengujian Hak Akses Bedasarkan *Role*:

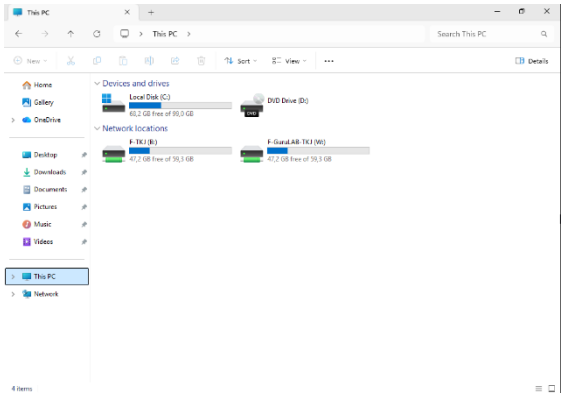


Pada gambar tersebut ditunjukkan proses login menggunakan akun adminsmk, yang memiliki hak administratif penuh untuk mengelola *Domain* dan mengakses seluruh folder pengguna.

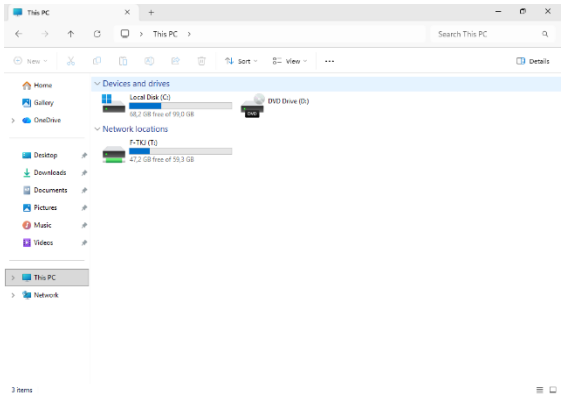


Gambar ini ditampilkan proses login menggunakan akun *StaffTU*, di mana pengguna

tersebut hanya diberikan hak akses terbatas sehingga hanya dapat membuka folder yang diperuntukkan bagi unit Tata Usaha saja.



Gambar ini ditunjukkan proses login menggunakan akun GuruLAB-TKJ, di mana pengguna tersebut memperoleh dua hak akses, yaitu akses ke folder GuruLAB-TKJ serta akses tambahan ke folder TKJ yang digunakan oleh siswa jurusan TKJ. Dengan hak akses tersebut, akun GuruLAB-TKJ dapat memantau dan mengawasi aktivitas yang berlangsung pada folder milik siswa TKJ sesuai kebutuhan pengelolaan kelas.



Gambar ini ditampilkan proses login menggunakan akun **siswa TKJ**, di mana pengguna tersebut hanya diberikan hak akses terbatas sehingga hanya dapat membuka folder yang diperuntukkan bagi siswa TKJ saja.

4.7 Monitoring

Pada tahap monitoring, dilakukan untuk mengevaluasi hasil penerapan sistem pengelolaan hak akses pengguna pada *Server* yang telah diimplementasikan. Pada penelitian ini, monitoring difokuskan pada pengujian penerapan *Role-Based Access Control* (RBAC) pada *Active Directory Domain Services* untuk memastikan bahwa kebijakan hak akses folder berjalan sesuai dengan peran pengguna yang telah ditentukan.

Tahap monitoring bertujuan untuk mengetahui sejauh mana sistem mampu membatasi akses pengguna terhadap folder yang tidak menjadi kewenangannya serta untuk membandingkan kondisi sistem sebelum dan sesudah penerapan RBAC. Monitoring dilakukan dengan cara melakukan pengujian langsung terhadap hak akses folder menggunakan akun pengguna yang mewakili setiap peran, yaitu siswa, guru, staf tata usaha, dan *administrator*.

4.7.1 Skenario Monitoring Hak akses folder

Skenario monitoring disusun berdasarkan kebijakan hak akses folder yang diterapkan pada *Server*. Penyusunan skenario ini dilakukan agar proses monitoring dapat mencerminkan kondisi penggunaan sistem yang sebenarnya di lingkungan sekolah.

Kebijakan hak akses folder yang digunakan dalam penelitian ini adalah sebagai berikut: akun siswa hanya diperbolehkan mengakses folder siswa, akun guru diperbolehkan mengakses folder guru dan folder siswa, akun staf tata usaha hanya diperbolehkan mengakses folder staf tata usaha, sedangkan akun administrator memiliki hak akses penuh terhadap seluruh folder yang terdapat pada *Server*.

Berdasarkan kebijakan tersebut, dilakukan pengujian terhadap 11 skenario akses folder yang melibatkan seluruh peran pengguna. Setiap skenario diuji untuk mengetahui kesesuaian hak akses yang diberikan oleh sistem. Skenario pengujian hak akses folder tersebut disajikan pada Tabel 4 – 5 berikut :

Tabel 4 Skenario Pengujian Hak Akses Folder Sebelum Implementasi

NO	Role Pengguna	Folder yang Diakses	Hak Akses Seharusnya	Sebelum RBAC	Keterangan
1	Siswa	Folder Siswa	Diizinkan	Diizinkan	Sesuai
2	Siswa	Folder Guru	Ditolak	Diizinkan	Pelanggaran

3	Siswa	Folder Staf TU	Ditolak	Diizinkan	Pelanggaran
4	Guru	Folder Siswa	Diizinkan	Diizinkan	Sesuai
5	Guru	Folder Guru	Diizinkan	Diizinkan	Sesuai
6	Guru	Folder Staf TU	Ditolak	Diizinkan	Pelanggaran
7	Staf TU	Folder Siswa	Ditolak	Diizinkan	Pelanggaran
8	Staf TU	Folder Guru	Ditolak	Diizinkan	Pelanggaran
9	Staf TU	Folder Staf TU	Diizinkan	Diizinkan	Sesuai
10	Administrator	Seluruh Folder	Diizinkan	Diizinkan	Sesuai
11	Administrator	Manajemen Hak Akses	Diizinkan	Diizinkan	Sesuai

Tabel 5 Skenario Pengujian Hak Akses Folder Sesudah Impelementasi

NO	Role Pengguna	Folder yang Diakses	Hak Akses Seharusnya	Sebelum RBAC	Keterangan
1	Siswa	Folder Siswa	Diizinkan	Diizinkan	Sesuai
2	Siswa	Folder Guru	Ditolak	Ditolak	Sesuai
3	Siswa	Folder Staf TU	Ditolak	Ditolak	Sesuai
4	Guru	Folder Siswa	Diizinkan	Diizinkan	Sesuai
5	Guru	Folder Guru	Diizinkan	Diizinkan	Sesuai
6	Guru	Folder Staf TU	Ditolak	Ditolak	Sesuai
7	Staf TU	Folder Siswa	Ditolak	Ditolak	Sesuai
8	Staf TU	Folder Guru	Ditolak	Ditolak	Sesuai
9	Staf TU	Folder Staf TU	Diizinkan	Diizinkan	Sesuai
10	Administrator	Seluruh Folder	Diizinkan	Diizinkan	Sesuai
11	Administrator	Manajemen Hak Akses	Diizinkan	Diizinkan	Sesuai

4.7.2 Hasil Monitoring Hak Akses Folder

Hasil monitoring diperoleh berdasarkan pengujian yang dilakukan terhadap seluruh skenario yang telah ditentukan. Pada kondisi sistem sebelum penerapan *Role-Based Access Control* (RBAC), masih ditemukan pengguna yang dapat mengakses folder yang tidak sesuai dengan perannya. Dari total 11 skenario pengujian, ditemukan sebanyak 6 skenario pelanggaran akses.

Setelah RBAC diterapkan, hasil monitoring menunjukkan bahwa sistem mampu membatasi seluruh akses yang tidak sesuai dengan peran pengguna. Pengguna hanya dapat mengakses folder yang menjadi haknya sesuai dengan kebijakan yang telah ditentukan, sehingga tidak ditemukan pelanggaran akses pada kondisi sistem setelah RBAC diterapkan.

4.7.3 Perhitungan *Violation Rate*

Untuk mengukur tingkat pelanggaran akses folder secara kuantitatif, dilakukan perhitungan *Violation Rate*. *Violation Rat*e digunakan untuk mengetahui persentase pelanggaran akses yang terjadi berdasarkan jumlah skenario pengujian yang dilakukan.
Perhitungan *Violation Rate* menggunakan rumus sebagai berikut:

$$\text{Violation Rate} = \frac{\textbf{\textit{Jumlah Pelanggaran}}}{\textbf{\textit{Jumlah Skenario Pengujian}}} \text{ x } 100\ \%$$

Berdasarkan hasil monitoring, jumlah skenario pengujian adalah sebanyak 11 skenario. Pada kondisi sistem sebelum penerapan RBAC ditemukan 6 pelanggaran akses, sehingga diperoleh nilai *Violation Rate* sebesar:

$$\frac{5}{11} \text{ x } 100\ \% = 45\ \%$$

Sedangkan pada kondisi sistem setelah penerapan RBAC tidak ditemukan pelanggaran

akses, sehingga nilai *Violation Rate* menjadi 0%. Hasil perhitungan tersebut menunjukkan bahwa penerapan *Role-Based Access Control* (RBAC) mampu menurunkan tingkat pelanggaran akses folder secara signifikan, sehingga sistem menjadi lebih aman dan terkontrol.

4.8 Manajemen

Pada tahap manajemen, dilakukan pengelolaan secara berkala terhadap sistem *Active Directory Domain Services* (AD DS) berbasis *Role-Based Access Control* (RBAC) untuk memastikan seluruh konfigurasi tetap berjalan efektif dan sesuai kebutuhan sekolah. Kegiatan ini meliputi pemeliharaan *Server Domain controller*, pembaruan kebijakan *Group Policy* (GPO), penyesuaian peran pengguna dalam *Organizational Unit* (OU), serta perbaikan konfigurasi apabila terjadi kendala seperti kesalahan autentikasi atau konflik hak akses. Selain itu, kebutuhan akses pengguna juga dievaluasi secara rutin agar sistem dapat terus dikembangkan dan disesuaikan dengan dinamika operasional di SMK Al-Badar. Dengan manajemen yang teratur, diharapkan sistem AD DS tetap stabil, aman, dan mampu mendukung aktivitas seluruh civitas akademika secara optimal.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mengenai implementasi *Role-Based Access Control* (RBAC) pada *Active Directory Domain Services* (AD DS) untuk manajemen ha8olpk akses pengguna di Server SMK Al-Badar, maka dapat ditarik kesimpulan sebagai berikut:

1. Penelitian ini berhasil mengimplementasikan *Role-Based Access Control* (RBAC) pada layanan *Active Directory Domain Services* berbasis *Windows Server* 2022 di lingkungan SMK Al-Badar melalui pembentukan struktur *Organizational Unit* (OU), grup keamanan, akun pengguna, serta penerapan *Group Policy Object* (GPO) sesuai dengan peran pengguna, yaitu *administrator*, guru, *staf* tata usaha, dan siswa. Implementasi ini memungkinkan pengelolaan akun dan hak akses dilakukan secara terpusat, terstruktur, dan sesuai dengan tugas serta tanggung jawab masing-masing pengguna.
2. Hasil pengujian menunjukkan bahwa penerapan RBAC pada AD DS mampu meningkatkan efektivitas pengelolaan hak akses pengguna di Server SMK Al-Badar. Sistem yang diterapkan berhasil membatasi akses yang tidak sesuai dengan peran pengguna, yang ditunjukkan oleh rendahnya tingkat pelanggaran akses *(violation rate)*. Selain itu, penerapan RBAC juga mempermudah proses monitoring dan administrasi jaringan, serta meningkatkan sistem informasi sekolah.
3. Kelebihan Sistem ini yaitu
   a. Manajemen Hak Akses Terpusat
   b. Pembagian Hak Akses Lebih Terstruktur dengan RBAC
   c. Peningkatan Keamanan Sistem Jaringan
   d. Efisiensi Administrasi dan Pengelolaan Akun
   e. Mendukung Monitoring dan Evaluasi Akses Pengguna
4. Kekurangan Sistem ini yaitu
   a. Ketergantungan pada Server Pusat
   b. Membutuhkan Administrator dengan Keahlian Khusus
   c. Kompleksitas Konfigurasi Awal
   d. Terbatas pada Lingkungan Windows
   e. Evaluasi Masih Terbatas pada Skenario Tertentu

1. UCAPAN TERIMA KASIH

Penulis Penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada dosen pembimbing, Bapak Arip Solehudin dan Bapak Carudin, atas bimbingan arahan, dan dukungan yang diberikan selama proses penelitian dan penulisan jurnal ini. Penulis juga menghargai segala bentuk bantuan, dukungan,dan motivasi dari berbagai pihak, baik secara langsung maupun tidak langsung, yang telah membantu terselesaikannya jurnal berjudul "Implementasi *Role-Based Access Contro*l (RBAC) Pada *Active Directory Domain Service* Untuk Manajemen Hak Akses Pengguna Di Server Smk Al-Badar."

Tanpadukungan dari semua pihak tersebut, penelitian ini tidak akan dapat terlaksana dengan baik. Semoga segala kebaikan dan bantuan yang diberikan mendapatkan balasan yang setimpal, serta hasil penelitian ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya dalam Jaringan Komputer.

DAFTAR PUSTAKA

[1] A. Jumarta, Z. R. Mair, dan M. Ramadhan, "Implementasi Active Directory Domain Controller pada Stasiun Meteorologi Sultan Mahmud Badaruddin II Palembang untuk pengelolaan akses dan keamanan data," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 4, pp. 5886–5888, 2025.

[2] G. M. Taberima dan D. Ramayanti, "Mengoptimalkan manajemen dan keamanan TI melalui implementasi layanan Domain Active Directory: Studi kasus pada infrastruktur TI perusahaan," *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, vol. 6, no. 1, pp. 79–89, 2024.

[3] J. L. Rizky dan 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. 2, pp. 51–53, 2022.

[4] A. W. Firmansyah, R. D. Marcus, A. S. Ilmananda, dan F. Y. Pamuji, "Manajemen akun pengguna berbasis roaming profile untuk memperkuat perlindungan data di laboratorium komputer," *SMATIKA: STIKI Informatika Jurnal*, vol. 12, no. 2, pp. 255–264, 2022.

[5] Haeruddin dan B. F. Pangaribuan, "Perancangan dan implementasi Active Directory Domain Controller menggunakan Windows Server 2012 R2 di PT Flextronics Technology Indonesia," dalam *Prosiding National Conference for Community Service Project (NaCosPro)*, vol. 3, no. 1, pp. 1150–1152, 2021.

[6] S. Hardiyansyah dan I. Zaenuddin, *Panduan Singkat Mengenal Lebih Dekat Active Directory Domain Services Windows Server 2022*. Jawa Barat, Indonesia: Penerbit Adanu Abimata, 2023.

[7] N. Sadikin dan 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, 2023.

[8] D. Tanjung dan 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, 2022.

[9] A. K. Nasich, S. A. Wicaksono, dan M. C. Saputra, "Implementasi role-based access control (RBAC) dalam sistem informasi manajemen pelanggan dan pembayaran air berbasis web," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 9, pp. xx–xx, 2025.

[10] R. W. Pratama, "Implementasi sistem autentikasi user menggunakan RADIUS server dan Active Directory pada jaringan wireless di PT Kudo Teknologi Indonesia," ResearchGate, 2019.

[11] A. S. Nugroho, "Sentralisasi otentikasi pengguna dan pengelolaan sumber daya jaringan komputer dengan Active Directory Domain Services Windows Server 2012 R2," in Prosiding SNITT Politeknik Negeri Balikpapan, Balikpapan, 2017.

[12] O. M. Dada, K. J. Adedotun, F. S. Oyedepo, dan A. K. Raji, "Leveraging role-based access control for secure and efficient result processing in academic environments," *Journal of Educational Studies, Trends and Practice*, vol. 6, no. 8, pp. 105–116, 2024.

[13] F. Naim, R. R. Saedudin, dan U. Y. K. S. Hediyanto, "Analysis of wireless and cable network quality-of-service performance at Telkom University Landmark Tower using Network Development Life Cycle (NDLC) method," *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika (JIPI)*, vol. 7, no. 4, 2022.

[14] N. Afif, "Manajemen akses dan direktori user dalam laboratorium TI UIN Alauddin Makassar berbasis Active Directory Windows," *Jurnal Manajemen Akses dan Direktori User*, vol. 1, no. 1, pp. 21–30, 2016.

[15] M. R. Santosa, Purwantoro, dan A. Suharso, "Perbandingan analisis manajemen bandwidth menggunakan metode simple queue dan queue tree pada Lawang Café Karawang," *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 12, no. 3, pp. 3261–3268, Aug. 2024, doi: 10.23960/jitet.v12i3.4961.