

Analisis Manajemen Sistem pada Sistem Operasi Windows

Muhamad Rizal – 11241049

Mata Kuliah: IF2514303 – Sistem Operasi

1. Manajemen Proses

Pada sistem operasi Windows, manajemen proses bertugas untuk mengatur pembuatan, penjadwalan, dan penghentian proses. Windows menggunakan *Windows Scheduler* untuk menentukan proses mana yang dijalankan oleh CPU. Windows menerapkan konsep *multitasking preemptive*, yang berarti CPU dapat mengganti proses sebelum proses yang sedang dijalankan selesai agar sistem terasa lebih responsif.

Adapun beberapa komponen penting pada manajemen proses adalah sebagai berikut:

- **Process Control Block (PCB)** berfungsi untuk menyimpan informasi penting seperti *Process ID, Process State, CPU Context, Memory Management, Scheduling Information, I/O Information, dan Security Info*. PCB memastikan sistem dapat melakukan *context switching* dengan cepat tanpa kehilangan status proses yang sedang berjalan.
- **Windows Task Manager** adalah alat yang digunakan untuk memantau dan mengelola proses yang sedang berjalan. Melalui *Task Manager*, pengguna dapat memantau kinerja sistem secara *realtime*, termasuk *CPU Usage, RAM Usage, Storage Activity, Network Activity*, serta status dari masing-masing proses. *User* juga dapat mengakhiri proses, mengatur prioritas, dan memantau performa sistem secara keseluruhan.
- **Windows Service** berfungsi sebagai kumpulan proses *background* yang berjalan tanpa antarmuka pengguna (*non-interactive*). Contohnya termasuk *Windows Update Service, Print Spooler, dan Windows Defender Service*. Layanan-layanan ini dikelola oleh *Service Control Manager (SCM)*, yang bertanggung jawab untuk memulai, menghentikan,

atau mengonfigurasi *service* sesuai kebutuhan sistem. Mereka sering berjalan dengan hak akses tinggi (*system-level privileges*) agar dapat mengakses komponen kernel atau *hardware*.

2. Manajemen Memori

Manajemen memori dalam sistem operasi Windows memiliki tugas untuk mengalokasikan dan mengatur ruang memori untuk proses agar tidak saling bertabrakan. Dalam penerapannya, Windows menggunakan *Virtual Memory System* yang memetakan *Physical Memory* (RAM) dan *Virtual Memory* di *page file*.

Adapun mekanisme yang digunakan oleh Windows untuk melakukan manajemen memori yaitu:

- **Paging** adalah proses memecah memori menjadi blok-blok kecil yang disebut *pages*. Sistem operasi kemudian memetakan halaman-halaman ini ke alamat virtual, sehingga aplikasi dapat menggunakan lebih banyak memori daripada yang tersedia secara fisik di RAM. Dengan *virtual memory*, Windows mampu menjaga agar sistem tetap responsif bahkan saat banyak aplikasi berjalan bersamaan.
- **Page File** digunakan ketika kapasitas RAM sudah tidak mencukupi. Windows menggunakan *Page File* (*pagefile.sys*) sebagai ekstensi dari memori fisik. File ini terletak di *hard drive* atau SSD dan berfungsi menyimpan data dari halaman memori yang tidak sedang aktif digunakan. Proses ini disebut *swapping*, dan memungkinkan sistem untuk meminjam ruang penyimpanan agar tidak kehabisan memori. Meskipun akses ke disk lebih lambat dibanding RAM, mekanisme ini mencegah aplikasi *crash* karena kekurangan memori.
- **Memory Protection** adalah sistem keamanan yang memastikan setiap proses hanya dapat mengakses ruang memorinya sendiri. Jika suatu proses mencoba membaca atau menulis ke memori milik proses lain, maka *Memory Management Unit* (MMU) akan mencegahnya, dan sistem dapat menghasilkan *error* seperti *Access Violation*. Mekanisme ini penting untuk mencegah kerusakan data dan menjaga stabilitas sistem.
- **Dynamic Link Library (DLL) Sharing** membuat Windows lebih efisien dalam penggunaan memori. DLL memungkinkan beberapa aplikasi menggunakan kode atau fungsi

yang sama tanpa perlu memuat salinan terpisah di memori masing-masing. Dengan begitu, sistem dapat menghemat RAM, mempercepat waktu *loading* aplikasi, dan memudahkan pembaruan fungsi karena cukup memperbarui satu file DLL saja.

3. Manajemen Storage

Manajemen *storage* berfungsi untuk mengatur penyimpanan data jangka panjang di media seperti *Hard Disk Drive (HDD)* atau *Solid State Drive (SSD)*. Windows menggunakan sistem file **NTFS (New Technology File System)** untuk mengelola file, direktori, serta metadata yang terkait.

Adapun fitur utama dalam NTFS antara lain:

- **File Permission & Encryption (EFS)** menjaga keamanan file dengan memberikan hak akses spesifik kepada pengguna tertentu dan mengenkripsi file agar tidak mudah dibuka oleh pihak yang tidak berwenang.
- **Journaling** berfungsi untuk mencegah kehilangan data saat sistem tiba-tiba mati atau mengalami *crash*. NTFS menyimpan catatan (*journal*) perubahan yang akan dilakukan, sehingga jika terjadi kegagalan, sistem dapat memulihkan struktur file dari log tersebut.
- **Compression & Quota** membantu menghemat ruang penyimpanan dengan melakukan kompresi file, serta memberikan batasan (*quota*) terhadap penggunaan disk oleh pengguna tertentu agar kapasitas penyimpanan dapat terkontrol.

4. Manajemen I/O

Manajemen *Input/Output (I/O)* bertugas menangani interaksi antara perangkat keras seperti *keyboard, mouse, printer, display, storage device* dan sistem operasi. Windows menggunakan **I/O Manager** yang berada di dalam kernel untuk mengatur aliran data antara perangkat dan sistem.

Adapun mekanisme utama pada manajemen I/O di Windows yaitu:

- **Device Driver** adalah modul perangkat lunak yang menerjemahkan perintah sistem operasi ke dalam bahasa yang dimengerti oleh perangkat keras. Setiap jenis perangkat memiliki *driver* tersendiri agar dapat berkomunikasi dengan sistem.
- **Plug and Play (PnP)** memungkinkan Windows untuk secara otomatis mengenali, menkonfigurasi, dan menginstal driver saat perangkat baru terhubung ke sistem tanpa memerlukan intervensi pengguna.

- **Buffering & Spooling** berfungsi menyimpan sementara data sebelum dikirim ke perangkat I/O seperti printer atau disk. Teknik ini membantu meningkatkan efisiensi dan menghindari penundaan dalam proses input/output.

5. Manajemen Keamanan

Manajemen keamanan bertugas melindungi sistem operasi dan data pengguna dari akses tidak sah serta ancaman keamanan lainnya. Windows memiliki **Windows Security Architecture** yang mencakup proses *authentication*, *authorization*, dan *auditing* untuk menjaga integritas sistem.

Fitur utama dalam manajemen keamanan Windows antara lain:

- **User Account Control (UAC)** mencegah perubahan sistem tanpa izin administrator dengan meminta konfirmasi setiap kali program mencoba melakukan modifikasi tingkat sistem.
- **Windows Defender / SmartScreen** berfungsi melindungi sistem dari *malware*, *spyware*, *phishing*, dan file berbahaya lainnya secara real-time.
- **NTFS Permission** memberikan kontrol akses terhadap file dan folder, menentukan siapa yang memiliki hak untuk membaca, menulis, atau menghapus file.
- **Encryption (BitLocker)** mengamankan seluruh drive dengan enkripsi penuh, memastikan data tetap terlindungi bahkan jika perangkat dicuri atau hilang.