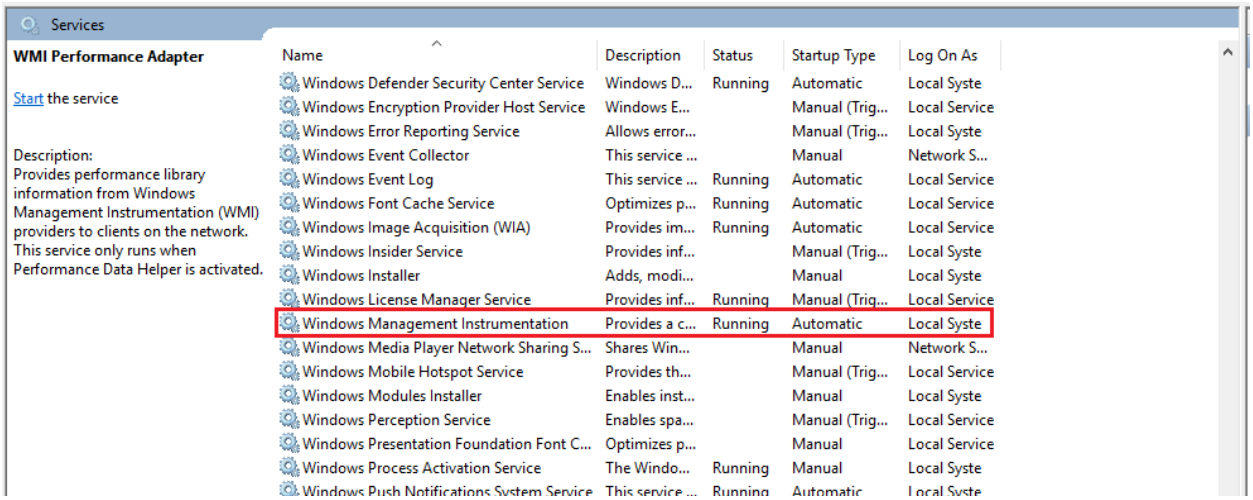
WMIچیست و چه کاربردی در مدیریت سیستم‌های ویندوزی در ۲۰۲۶ دارد؟

WMI چیست و چه کاربردی در مدیریت سیستم‌های ویندوزی دارد؟ در مسیر اجرای پروژه‌های نرم‌افزاری و زیرساختی، بارها با این نیاز مواجه می‌شویم که به اطلاعات دقیق و ساخت‌یافته‌ای از سیستم‌عامل، سخت‌افزار و نرم‌افزارهای نصب‌شده بر روی یک سیستم ویندوزی دسترسی داشته باشیم. این اطلاعات می‌توانند نقش کلیدی در مانیتورینگ، عیب‌یابی، اتوماسیون، گزارش‌گیری و مدیریت متمرکز سیستم‌ها ایفا کنند. در نگاه نخست، ممکن است استفاده از زبان‌های برنامه‌نویسی سطح پایین مانند C یا C++ به‌عنوان راه‌حل به ذهن برسد؛ اما پیاده‌سازی چنین راهکارهایی معمولاً زمان‌بر، پرهزینه و پیچیده است و نگهداری آن‌ها در پروژه‌های سازمانی توجیه فنی و اقتصادی مناسبی ندارد.

مایکروسافت برای پاسخ به این نیاز، قابلیتی قدرتمند را به‌صورت یک سرویس داخلی در سیستم‌عامل Windows فراهم کرده است که امکان دسترسی استاندارد، امن و ساخت‌یافته به اطلاعات سیستم را فراهم می‌کند. این سرویس، بدون نیاز به توسعه کدهای سطح پایین، بستری یکپارچه برای مدیریت و مانیتورینگ منابع ویندوز در اختیار توسعه‌دهندگان و مدیران سیستم قرار می‌دهد. در این مقاله، قصد داریم به معرفی این سرویس یعنی WMI (Windows Management Instrumentation) بپردازیم و با نقش، کاربردها و جایگاه آن در پروژه‌های واقعی آشنا شویم.



WMI چیست؟

WMI (Windows Management Instrumentation) یکی از اجزای اصلی و زیرساختی سیستم‌عامل Microsoft Windows است که به‌عنوان یک فریم‌ورک استاندارد برای مدیریت، مانیتورینگ و جمع‌آوری اطلاعات سیستم عمل می‌کند. این فناوری امکان دسترسی یکپارچه و ساخت‌یافته به اطلاعات مربوط به سخت‌افزار، سیستم‌عامل، سرویس‌ها، پردازش‌ها، تنظیمات امنیتی و نرم‌افزارهای نصب‌شده را فراهم می‌سازد.

WMI به‌صورت یک سرویس داخلی (Service) در ویندوز اجرا می‌شود و واسطی بین سیستم‌عامل و ابزارهای مدیریتی، اسکریپت‌ها و نرم‌افزارهای مانیتورینگ ایجاد می‌کند. به بیان ساده، WMI زبان مشترکی است که ویندوز از طریق آن وضعیت داخلی خود را گزارش می‌دهد و امکان مدیریت هوشمند سیستم را فراهم می‌سازد.

WMI چه مشکلی را حل می‌کند و کاربرد آن چیست؟

کاربرد عملی	WMIچگونه این مشکل را حل می‌کند	مشکل در مدیریت سیستم‌های ویندوزی
دریافت مشخصات CPU، RAM، Disk، Network	ارائه یک Interface استاندارد برای دسترسی به اطلاعات سیستم	نبود دسترسی متمرکز به اطلاعات سیستم
کاهش هزینه و زمان توسعه ابزارهای مدیریتی	انتزاع پیچیدگی‌های سطح پایین سیستم عامل	نیاز به استفاده از کدهای Low-Level (C/C++)
مانیتورینگ منابع در سازمان‌ها	فراهم‌کردن Queryهای ساخت‌یافته و قابل Automation	دشواری مانیتورینگ در مقیاس Enterprise
عملکرد صحیح SCCM، System Center	ایجاد یک لایه مشترک بین ابزارها و سیستم عامل	عدم یکپارچگی ابزارهای مدیریتی
Automation عملیات IT	امکان Integration با PowerShell و اسکریپت‌ها	مدیریت دستی و غیرقابل اتوماسیون
Health Checkو Troubleshooting	دسترسی Real-Time و Query-Based به داده‌ها	نبود دید دقیق نسبت به وضعیت سیستم‌ها
Azure Arc، Cloud Monitoring	پشتیبانی از Agentها و ابزارهای Cloud	چالش مدیریت سیستم‌های Hybrid (Cloud + On-Prem)

WMIچگونه کار می‌کند؟

WMI بر پایه مفهومی به نام Object-Oriented Management طراحی شده است. در این مدل:

- هر جزء از سیستم (مانند CPU، Disk، Process، Service و ...) به‌صورت یک Object تعریف می‌شود.
- این Objectها در قالب Classهایی ساخت‌یافته، اطلاعات خود را در اختیار WMI قرار می‌دهند.
- ابزارها و اسکریپت‌ها می‌توانند از طریق Query (معمولاً با زبان WQL) به این اطلاعات دسترسی پیدا کنند.

WMI از استاندارد صنعتی CIM (Common Information Model) پیروی می‌کند که باعث می‌شود ساختار اطلاعات آن منسجم، قابل پیش‌بینی و قابل گسترش باشد.

WMI در چه سناریوهایی استفاده می‌شود؟

WMI یکی از پرکاربردترین و حیاتی‌ترین ابزارها در اکوسیستم سیستم‌عامل ویندوز محسوب می‌شود و در طیف گسترده‌ای از سناریوهای عملیاتی و سازمانی مورد استفاده قرار می‌گیرد. این فناوری به مدیران سیستم، تیم‌های IT و ابزارهای مدیریتی اجازه می‌دهد تا با کمترین سربار و بیشترین دقت، وضعیت سیستم‌ها را بررسی و مدیریت کنند.

از جمله مهم‌ترین کاربردهای WMI می‌توان به مانیتورینگ سیستم‌ها در مقیاس سازمانی اشاره کرد؛ جایی که اطلاعات مربوط به مصرف منابع، وضعیت سرویس‌ها و سلامت سیستم‌ها به‌صورت متمرکز جمع‌آوری می‌شود. همچنین WMI نقش کلیدی در اتوماسیون وظایف مدیریتی ایفا می‌کند و امکان اجرای اسکریپت‌ها و فرآیندهای خودکار را، به‌ویژه از طریق PowerShell، فراهم می‌سازد.

علاوه بر این، WMI بستری مناسب برای گزارش‌گیری دقیق از وضعیت سخت‌افزار و نرم‌افزار فراهم می‌کند و در سناریوهای مدیریت ریموت سیستم‌های ویندوزی به‌طور گسترده مورد استفاده قرار می‌گیرد. بسیاری از ابزارهای حرفه‌ای و سازمانی مایکروسافت و شرکت‌های ثالث، از جمله System Center، SCCM، ابزارهای Monitoring و راهکارهای EDR، به‌صورت مستقیم یا غیرمستقیم بر WMI متکی هستند.

توضیح	سناریو
جمع‌آوری و تحلیل اطلاعات مربوط به مصرف CPU، RAM، Disk، وضعیت سرویس‌ها و سلامت کلی سیستم‌ها	مانیتورینگ سیستم‌ها در مقیاس سازمانی
اجرای اسکریپت‌های مدیریتی و خودکارسازی فرآیندها با استفاده از PowerShell و سایر Scriptها	اتوماسیون وظایف مدیریتی
استخراج اطلاعات دقیق درباره مشخصات سخت‌افزاری، نرم‌افزارهای نصب‌شده و تنظیمات سیستم	گزارش‌گیری از وضعیت سخت‌افزار و نرم‌افزار
مشاهده، کنترل و مدیریت سیستم‌ها از راه دور بدون نیاز به دسترسی فیزیکی	مدیریت ریموت سیستم‌های ویندوزی
به‌کارگیری WMI به‌عنوان هسته اطلاعاتی در ابزارهایی مانند System Center، SCCM، Monitoring Tools و EDRها	استفاده در ابزارهای حرفه‌ای سازمانی

مزایا و معایب سرویسWMI

مزایایWMI	معایبWMI
دسترسی متمرکز و ساخت‌یافته به اطلاعات سیستم‌عامل، سخت‌افزار و نرم‌افزار	پیچیدگی مفهومی برای کاربران تازه‌کار

معایبWMI	مزایایWMI
سربار عملکردی در اجرای Queryهای سنگین یا مکرر	کاهش نیاز به توسعه کدهای سطح پایین مانند C و C++
عیب‌یابی و Debug دشوارتر نسبت به APIهای ساده	مستقل از زبان برنامه‌نویسی و قابل استفاده در PowerShell، C# و ابزارهای مدیریتی
وابستگی شدید ابزارها به سلامت سرویس WMI	مناسب برای مانیتورینگ و مدیریت در مقیاس سازمانی
ریسک‌های امنیتی در صورت پیکربندی نادرست دسترسی‌ها	پشتیبانی از مدیریت و مانیتورینگ ریموت سیستم‌های ویندوزی
محدودیت ذاتی به سیستم‌عامل Windows	یکپارچگی کامل با ابزارهای مایکروسافت مانند System Center و SCCM
عملکرد ضعیف‌تر در مقایسه با روش‌های مدرن‌تر در برخی سناریوها	مبتنی بر استاندارد CIM و قابل توسعه برای سناریوهای سفارشی

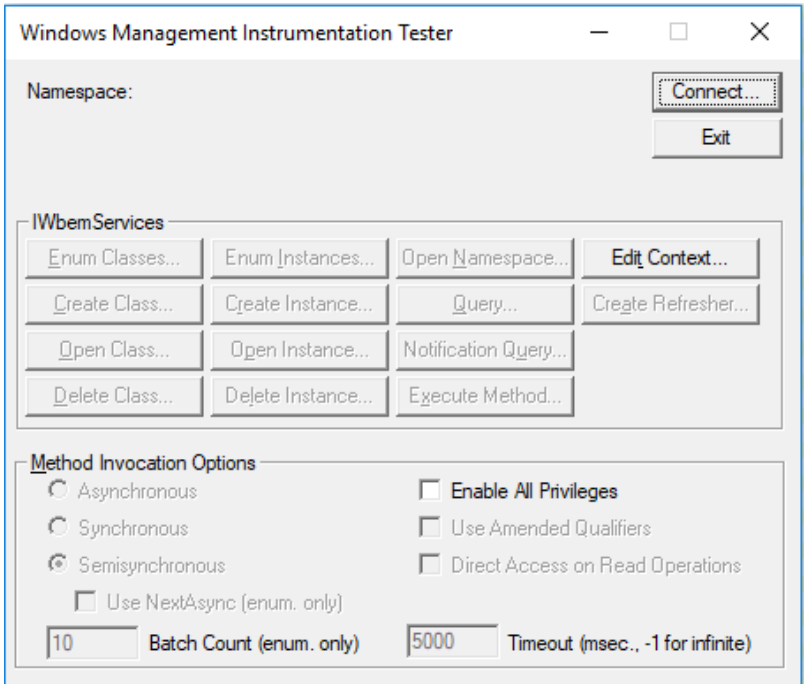
چگونه با WMI اطلاعات سخت‌افزار را دریافت کنیم؟

سرویس WMIبه عنوان بخشی از سیستم عامل، به شما اجازه می‌دهد تا اطلاعات مختلفی را مانند بخش‌های زیر بدست آورید:

- Win۳۲ Provider
- Event Log Provider
- Registry Provider
- Performance Counter Provider
- Active Directory Provider
- Windows Installer Provider

مثلا در خصوص بدست آوردن اطلاعات سخت افزار شما می‌توانید با یک دستور ساده اطلاعات زیر را بدست آورید:

- HDD Serial Number
- HDD Sizes
- HDD Free Space
- Network Adapter MAC Address
- Network Adapter Default Gateway



اگر بخواهیم ابزاری برای تست به شما معرفی کنیم ابزاری به نام WBEM Test وجود دارد که می‌توانید به اطلاعات این پایگاه داده دسترسی داشته باشید.برای دسترسی به برنامه WBEM Test کافی است برنامه RUNرا باز کنید و دستور wbemtest را درون آن اجرا کنید.

نکات امنیتی مهم (Windows Management Instrumentation) WMI در ویندوز

موضوع	توضیح / ریسک اصلی	توصیه امنیتی(Best Practice)
دسترسی پیش‌فرضRemote	فقط Administrators می‌توانند از راه دور به WMIدسترسی داشته باشند، اما همین کافی است برای Lateral Movement	فقط حساب‌های ضروری را در گروه Distributed COM UsersیاWMI Remote Enableبگذارید) اصل Least Privilege)
امنیت Namespaceها	هر namespace امنیت جداگانه دارد) مثلroot\cimv۲ ، root\subscriptionو(...	از) WMI Controlدر (mmc یا PowerShellامنیتnamespace ها را سخت‌گیرانه تنظیم کنید – دسترسی Execute Methodsو Remote Enable را محدود کنید
WMI Event Subscription (T۱۵۴۶.۰۰۳)	مهاجم می‌تواند Event Filter + Consumer + Bindingبسازد → اجرای کد با SYSTEM بعد از Reboot	مرتب root\subscription را چک کنید) با Autorunsیا Event .(PowerShell های مشکوک را حذف کنید. دسترسی به این namespaceرا خیلی محدود کنید
سوءاستفاده از WMICو Impacket	WMICهنوز در خیلی سیستم‌ها فعال است و ابزارهایی مثل wmiexec.pyخیلی استفاده می‌شود	WMICرا در سیستم‌های جدید غیرفعال کنید) از ۲۰۲٤ در Windows ۱۱ Insider پیش‌فرض خاموش است .(از AMSI و EDR برای تشخیص استفاده کنید
RPC وDCOM Ports	WMIاز DCOM/RPC استفاده می‌کند → پورت‌های داینامیک بالا باز می‌شوند	فایروال را سخت‌گیرانه کنید. فقط ازIP های مجاز) مثلاً SCCM server اجازه WMI Remoteبدهید. از Kerberos استفاده کنید نهNTLM
لاگ و مانیتورینگ ضعیف	فعالیت‌های WMI به راحتی دیده نمی‌شود مگر با تنظیم درست auditing	Event IDهای مهم WMI را مانیتور کنید)مثل ۵۸۵۹, ۵۸۶۰, ۵۸۶۱ در + Security Microsoft-Windows-WMI-Activity/Operational)

توصیه امنیتی(Best Practice)	توضیح / ریسک اصلی	موضوع
WMI Repositoryرا بک‌آپ بگیرید (winmgmt /salvagerepository)یا /resetrepositoryدر مواقع اضطراری .(Integrityچک کنید	مهاجم می‌تواند Repository را دستکاری کند یا برای Persistence استفاده کند	Repositoryخراب یا دستکاری‌شده
حساب‌های Service را با حداقل دسترسی تنظیم کنید. از GPO برای اعمال Baseline امنیتی WMI استفاده کنید	SCCM، SCOM، Azure Arc، Intune، Monitoring Agentها همه به WMI وابسته‌اند	استفاده در ابزارهای مدیریتی
ویندوز و .NET Framework را همیشه به‌روز نگه دارید. CIS Benchmarks بخش WMIرا اعمال کنید	آسیب‌پذیری‌های قدیمی در WMI و وابستگی‌هایش هنوز وجود دارد	عدم پچ و به‌روزرسانی

آشنایی باWMI Repository

WMI Repositoryدر واقع قلب *پایگاه داده‌ای* Windows Management Instrumentation است؛ محلی که تمام اطلاعات مدیریتی ویندوز به‌صورت ساخت‌یافته در آن نگهداری می‌شود. هر زمان که شما از طریق) WMI مثلاً باPowerShell ، WBEM Testیا ابزارهای مدیریتی سازمانی (درخواستی برای دریافت اطلاعات سیستم ارسال می‌کنید، این درخواست در نهایت به Repository ارجاع داده می‌شود.

WMI Repository دقیقاً چه چیزی را نگهداری می‌کند؟

WMI Repository شامل مجموعه‌ای از Classها، Namespaceها و Provider Registrationها است که اطلاعات زیر را پوشش می‌دهد:

- ساختار کلاس‌های WMI (مانند Win۳۲_Processor، Win۳۲_LogicalDisk)
- ارتباط بین Providerها و داده‌های سیستم
- متادیتای مربوط به سخت‌افزار، سیستم‌عامل و سرویس‌ها
- اطلاعات Performance Counterها
- داده‌های مرتبط با Event Log، Registry و Installer

به زبان ساده: Repository نقشه‌ی کامل اطلاعات مدیریتی ویندوز است.

ارتباط WMI Repository با Providerها

Providerها (مثل Win۳۲ Provider یا Event Log Provider) منبع داده نیستند، بلکه واسطه‌اند.

فرآیند به این شکل است:

۱. درخواست Query (مثلاً WQL یا PowerShell) ارسال می‌شود
۲. WMI Service درخواست را دریافت می‌کند
۳. Repository مشخص می‌کند:
   - کدام Class
   - توسط کدام Provider
۴. Provider داده واقعی را از سیستم جمع‌آوری می‌کند
۵. نتیجه به کاربر یا ابزار مدیریتی بازگردانده می‌شود

نقش WMI Repository در ابزار WBEM Test

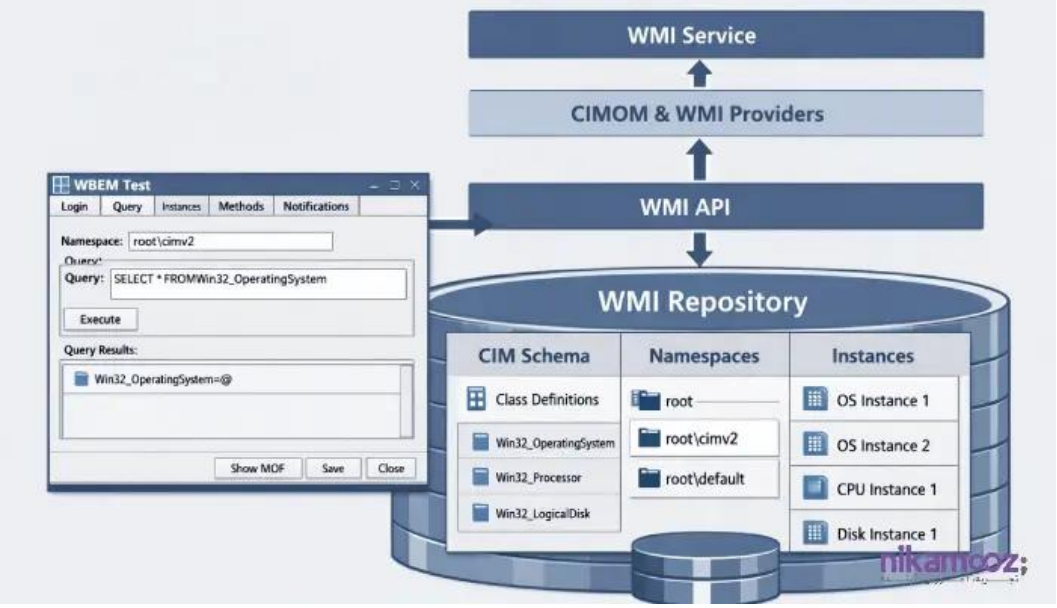
ابزار WBEM Test در حقیقت یک رابط مستقیم برای بررسی محتوای WMI Repository است.

با استفاده از WBEM Test شما می‌توانید:

- Namespaceها را مشاهده کنید (مثل root\cimv۲)
- Classهای موجود در Repository را بررسی کنید
- Query مستقیم روی Repository اجرا کنید
- صحت و سلامت داده‌های WMI را تست کنید

به همین دلیل، WBEM Test یکی از ابزارهای کلیدی برای:

- عیب‌یابی WMI
- بررسی Providerها
- تحلیل مشکلات مانیتورینگ محسوب می‌شود.



محل ذخیره‌سازی WMI Repository در ویندوز

Repository به‌صورت فیزیکی در مسیر زیر ذخیره می‌شود:

C:\Windows\System۳۲\wbem\Repository

این پوشه شامل فایل‌هایی است که:

- ساختار Classها
- Mapping Providerها
- و داده‌های کش‌شده WMI

را نگهداری می‌کنند.

⚠️ هرگونه آسیب به این Repository می‌تواند باعث:

- خطا در Queryهای WMI
- از کار افتادن ابزارهای مدیریتی
- اختلال در Performance Monitoring شود.

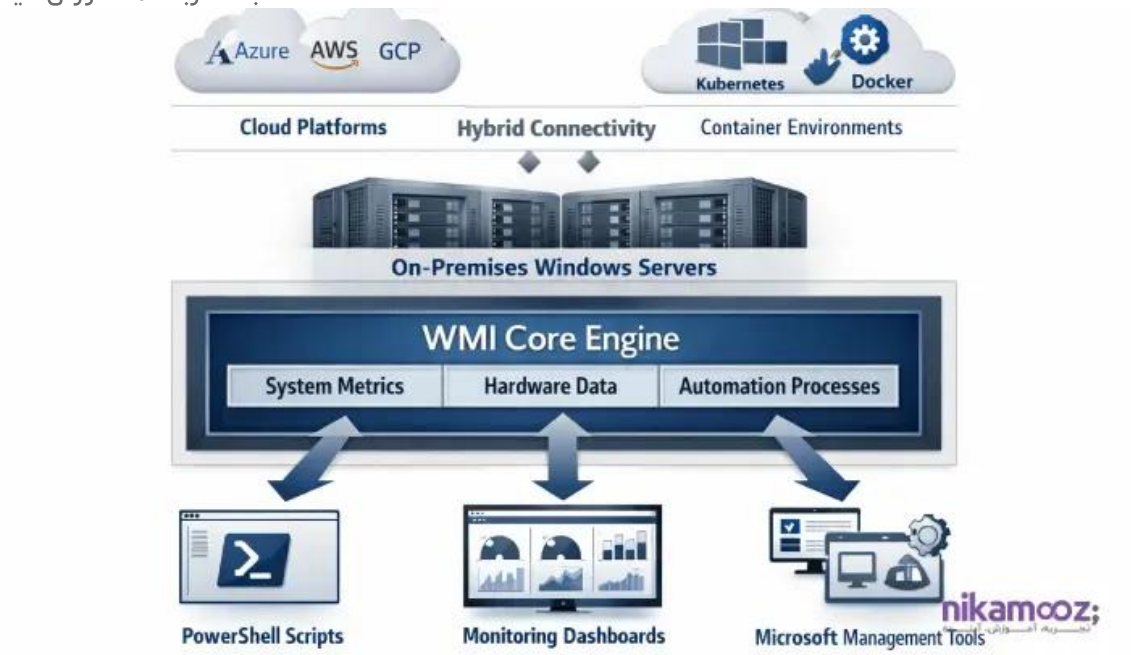
چرا سلامت WMI Repository اهمیت حیاتی دارد؟

مؤلفه	توضیح
نقش WMI Repository	پایگاه مرکزی اطلاعات مدیریتی ویندوز که ابزارها و اسکریپت‌ها برای دریافت داده به آن متکی هستند
System Center	برای جمع‌آوری وضعیت سیستم‌ها، سرویس‌ها و Compliance به WMI Repositoryوابسته است
SCCM	Inventoryسخت‌افزار و نرم‌افزار، Discoveryو Reporting از طریق WMI انجام می‌شود
Monitoring Solutions	ابزارهای مانیتورینگ(CPU ، Disk، Network، Serviceداده‌ها را از WMI استخراج می‌کنند
PowerShell Automation	بسیاری ازCmdlet ها و اسکریپت‌های مدیریتی مستقیماًQuery های WMI اجرا می‌کنند
Cloud Agentها (Hybrid)	Agentهای Cloud / Azure برای Sync اطلاعات On-Prem به Cloud به WMIوابسته‌اند
پیامد خرابی Repository	اختلال درQuery ها، خطا در مانیتورینگ، ناتوانی ابزارهای مدیریتی
نتیجه نگهداری صحیح	پایداری زیرساخت، مانیتورینگ دقیق، Automationقابل اعتماد

چرا WMI همچنان مهم است؟

با وجود حرکت دنیای IT به سمت Cloud و Container، WMI همچنان هسته مدیریت ویندوز محسوب می‌شود و بسیاری از ابزارهای مدرن مایکروسافت، به‌صورت مستقیم یا غیرمستقیم، بر آن تکیه دارند.

برای SysAdminها، IT Proها و Cloud Engineerهایی که با محیط‌های Hybrid و *Windows-based* سروکار دارند، شناخت WMI یک دانش پایه اما حیاتی محسوب می‌شود.



سخن پایانیWMI

WMI (Windows Management Instrumentation)زیرساخت اصلی و استاندارد مدیریت و مانیتورینگ در ویندوز است که به مدیران سیستم و ابزارها امکان دسترسی ساخت‌یافته، امن و یکپارچه به تقریباً تمام اطلاعات سیستم (سخت‌افزار، نرم‌افزار نصب‌شده، سرویس‌ها، پروسس‌ها، تنظیمات، لاگ‌ها، عملکرد و ...) را بدون نیاز به کدنویسی سطح پایین می‌دهد. این سرویس با استفاده از مدل شیءگرا و استاندارد CIM کار می‌کند، از طریق PowerShell و WQL قابل کوئری‌نویسی است و پایه بسیاری از ابزارهای سازمانی مانندSCCM ، System Center، SCOM، Azure Arcو اکثر راهکارهای مانیتورینگ و EDR محسوب می‌شود. با وجود مزایای بزرگ مانند اتوماسیون قوی و مدیریت ریموت، چالش‌های امنیتی آن) به‌ویژه در دسترسی ریموت وnamespace های حساس (و سربار عملکردی در کوئری‌های سنگین، همچنان در سال ۲۰۲۶ یکی از اجزای کلیدی و تقریباً اجتناب‌ناپذیر هر محیط ویندوزی On-Prem یا Hybrid به شمار می‌رود.

سوالات متداولWMI

۱. WMIچیست؟

WMIیا Windows Management Instrumentation یک زیرساخت داخلی ویندوز است که دسترسی استاندارد، ساخت‌یافته و امن به اطلاعات سیستم‌عامل، سخت‌افزار، سرویس‌ها، پروسس‌ها و نرم‌افزارهای نصب‌شده فراهم می‌کند.

۲. WMIچه مشکلی را در مدیریت سیستم‌های ویندوزی حل می‌کند؟

مشکل نبود دسترسی متمرکز، یکپارچه و آسان به اطلاعات دقیق سیستم را حل می‌کند و نیاز به نوشتن کدهای پیچیده سطح پایین (مثل C/C++) را از بین می‌برد.

۳. مهم‌ترین کاربردهای WMI در محیط‌های سازمانی چیست؟

مانیتورینگ منابع سیستم در مقیاس بزرگ، اتوماسیون وظایف باPowerShell، گزارش‌گیری از سخت‌افزار و نرم‌افزار، مدیریت ریموت سیستم‌ها و تأمین داده برای ابزارهایی مثل SCCM، System Center و راهکارهای EDR.

٤. چگونه می‌توان با WMI اطلاعات سخت‌افزاری مثل سریال هارد یا مشخصات شبکه را به دست آورد؟

از طریق کوئری روی کلاس‌های WMI (مثل Win۳۲_LogicalDisk یا Win۳۲_NetworkAdapter)با ابزارهایی مثل PowerShell یا wbemtest می‌توان این اطلاعات را استخراج کرد.

٥. WMI Repositoryچیست و کجا قرار دارد؟

WMI Repositoryپایگاه داده اصلی WMI است که تمام کلاس‌ها، namespaceها و اطلاعات مدیریتی را نگه می‌دارد و به‌صورت فیزیکی در مسیر C:\Windows\System۳۲\wbem\Repository ذخیره می‌شود .

٦. چرا امنیت WMI بسیار مهم است و چه ریسک‌هایی دارد؟

اگر درست پیکربندی نشود، امکان Lateral Movement، Persistence و اجرای کد با دسترسی SYSTEM توسط مهاجم وجود دارد؛ به‌خصوص از طریق WMI Event Subscription یا دسترسی ریموت غیرمجاز.

۷. آیا WMI هنوز در سال‌های جدید (مثل ۲۰۲۶) اهمیت دارد؟

بله، WMIهمچنان هسته اصلی مدیریت ویندوز است و ابزارهای مدرن مایکروسافت (SCCMها، Intune، Azure Arc، Monitoring Agent) و محیط‌های Hybrid به شدت به آن وابسته‌اند.

کسب اطلاعات بیشتر:

- *معرفی Performance Monitor ابزار مانیتورینگ SQL Server*
- *سرویس SQL Server Browser چیست؟ آشنایی با نحوه راه اندازی و کاربردها*
- *نصب آپاچی کافکا مرحله به مرحله؛ از پیکربندی تا بهینه‌سازی*
- *ابزارهای مانیتورینگ | SQL Server معرفی، مقایسه و انتخاب بهترین ابزار*