WMI (Windows Management Instrumentation)

WMI je základní technologie pro správu operačního systému Windows. Jde o implementaci standardů WBEM (Web-Based Enterprise Management) a CIM (Common Information Model) od společnosti Microsoft. V jednoduchosti slouží WMI jako prostředník, který umožňuje správcům a aplikacím dotazovat se na stav systému a ovládat jej.

Jak WMI funguje?

WMI si lze představit jako rozsáhlou databázi informací o počítači, ke které lze přistupovat pomocí dotazovacího jazyka **WQL** (WMI Query Language), který je velmi podobný standardnímu SQL.

Pomocí WMI lze zjistit téměř cokoli o hardware i software:

- **Hardware:** Teplota procesoru, sériové číslo základní desky, kapacita disků.
- **Software:** Seznam nainstalovaných aplikací, běžící procesy, stav služeb.
- **Nastavení:** Konfigurace sítě, uživatelské účty, záznamy v registru.

Využití v rámci IT Podpory

V naší firmě využívá IT Podpora WMI především pro tyto účely:

Oblast	Praktické využití
Inventarizace	Automatický sběr dat o stáří a konfiguraci PC do naší evidence majetku.
Monitoring	Sledování vytížení serverů a volného místa na discích v reálném čase.
Automatizace	Hromadná instalace softwaru nebo vzdálené vypínání stanic (v kombinaci s WOL).
Troubleshooting	Vzdálená diagnostika chyb bez nutnosti fyzického přístupu k počítači.

WMI a Kybernetická bezpečnost

Protože WMI umožňuje hluboký přístup do systému, je kritickým bodem pro kybernetickou bezpečnost:

- **Vzdálený přístup:** WMI může fungovat přes síť (RPC), což vyžaduje přísné nastavení firewallu.
- **Oprávnění:** K dotazování na citlivé informace jsou vyžadována administrátorská práva.
- **Detekce útoků:** Útočníci mohou WMI zneužít k persitenci (udržení se v systému). Naše monitorovací systémy sledují podezřelé WMI dotazy.

Praktická ukázka (PowerShell)

Moderní správa WMI probíhá nejčastěji přes PowerShell. Příklad dotazu na model počítače a verzi

BIOSu:

```
Get-CimInstance -ClassName Win32_ComputerSystem | Select-Object Model,
Manufacturer
Get-CimInstance -ClassName Win32_BIOS | Select-Object SerialNumber,
SMBIOSBIOSVersion
```

> **Poznámka:** Microsoft postupně nahrazuje starší WMI příkazy (`Get-WmiObject`) modernějšími a bezpečnějšími variantami **CIM** (`Get-CimInstance`), které používají protokol WS-Man namísto DCOM. V rámci našeho vývoje skriptů preferujeme variantu CIM.

— **Související stránky:** IT Podpora, ZIF, Kybernetická bezpečnost, WOL, Vývojový tým

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=wmi

Last update: **2026/01/01 15:50**