Windows Management Instrumentation (WMI)

Jeff Hicks
AUTHOR ~ TEACHER ~ SENSEI
@jeffhicks https://jdhitsolutions.com/blog

What Is WMI?

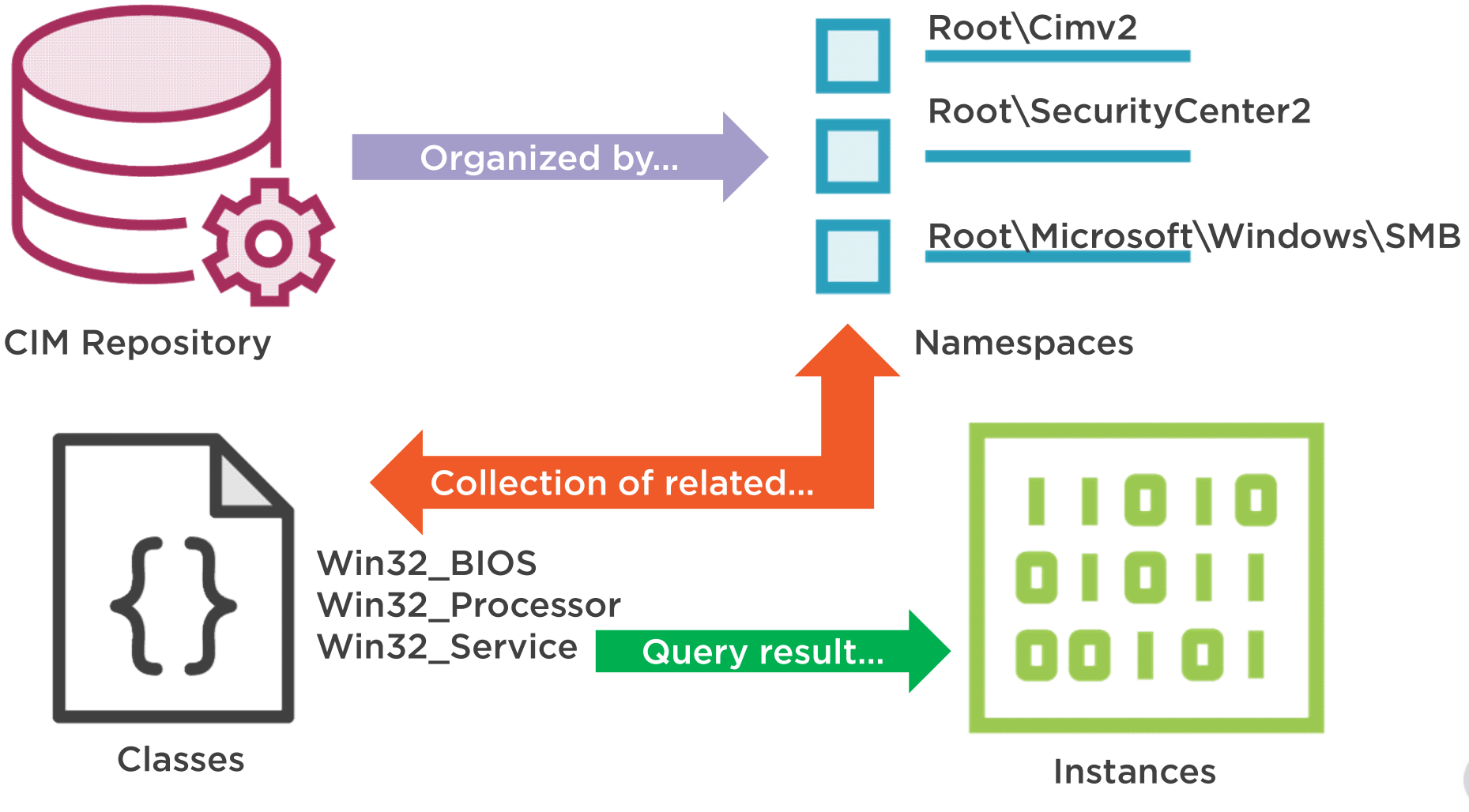
Local repository for system information

Managed by the winmgmt service

Can be queried with a SQL-like syntax

WMI is Microsoft's implementation

Derived from an industry set of standards


Root\Cimv2
Root\SecurityCenter2
Root\Microsoft\Windows\SMB
Organized by...
CIM Repository
Namespaces
Collection of related...
Win32_BIOS
Win32_Processor
Win32_Service
Query result...
Classes
Instances

```
Get-WmiObject –classname win32_service –computername SRV1
```

WMI Cmdlets

Easy to query local and remote computers

```
Get-WmiObject –classname win32_service –computername SRV1
–credential company\administrator
```

WMI Cmdlets

Easy to query local and remote computers

Supports alternate credentials for remote connections

Uses legacy networking protocols (not firewall friendly)

```
ExitCode  : 0
Name      : AdobeFlashPlayerUpdateSvc
ProcessId : 0
StartMode : Manual
State     : Stopped
Status    : OK
```

A rich, PowerShell object

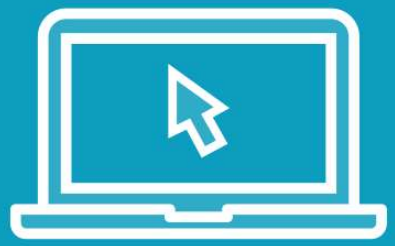
WMI Cmdlets

Easy to query local and remote computers

Supports alternate credentials for remote connections

Uses legacy networking protocols (not firewall friendly)

Demo



PowerShell and WMI

Summary

- WMI-based information is vital to systems management
- WMI cmdlets are supported for legacy systems
- Plan on moving to modern CIM cmdlets