

Windows Monitoring with WMI and Powershell in GroundWork Monitor

Windows Monitoring with WMI and Powershell in GroundWork Monitor

WMI?

Powershell?

How to use these for Windows monitoring?
What are my choices?

What is WMI?

Windows Management Instrumentation (WMI)

Access to remote performance counters

Available and Enabled by default

What is Powershell?

Windows Command-line Shell

Scripting Language based on .NET

Needs to be Downloaded and Installed

(except on Windows Server 2008 R2 and Windows 7)

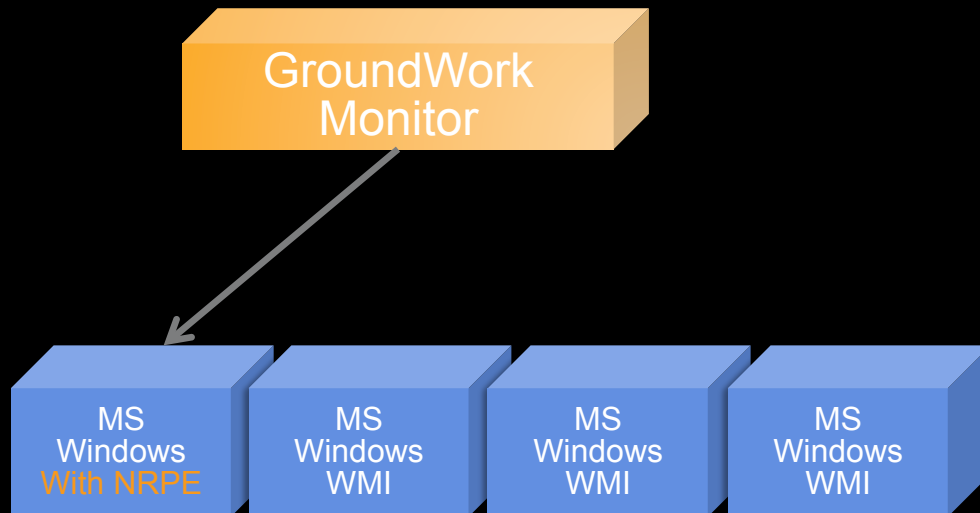
What is WinRM?

WS-Management Protocol for Windows
SOAP-based systems management
Must be enabled and secured

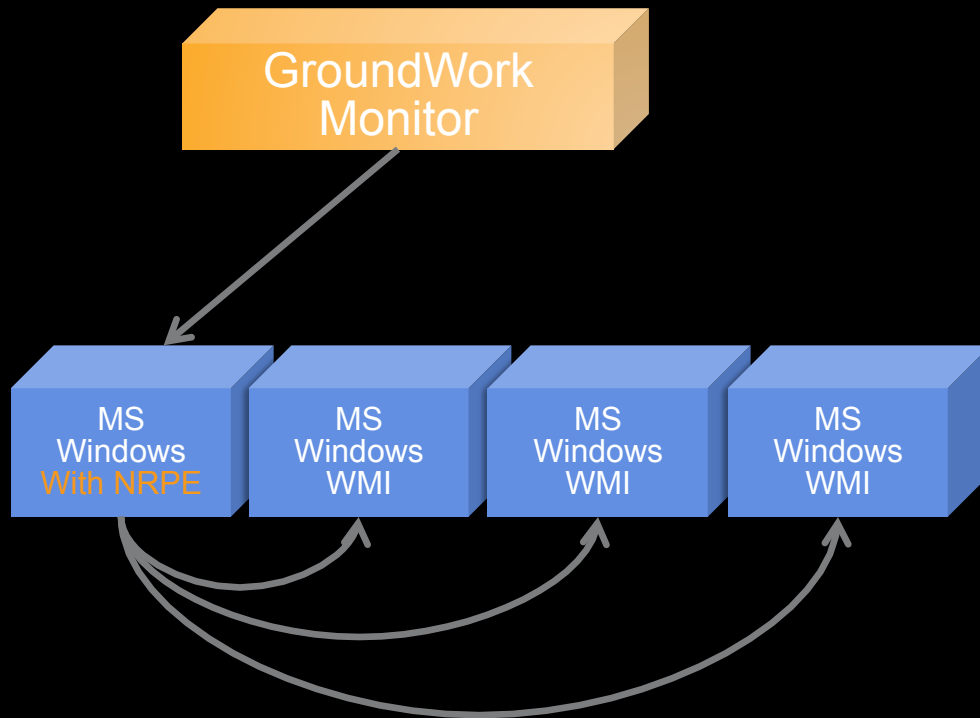
Windows Monitoring with WMI



Windows Monitoring with WMI



Windows Monitoring with WMI



Using WMI...

```
cscript.exe //nologo get_computer_info.vbs -h localhost -i logical_disks
```

```
Host name: ad; Logical Disks: A:, C:, D:,
```

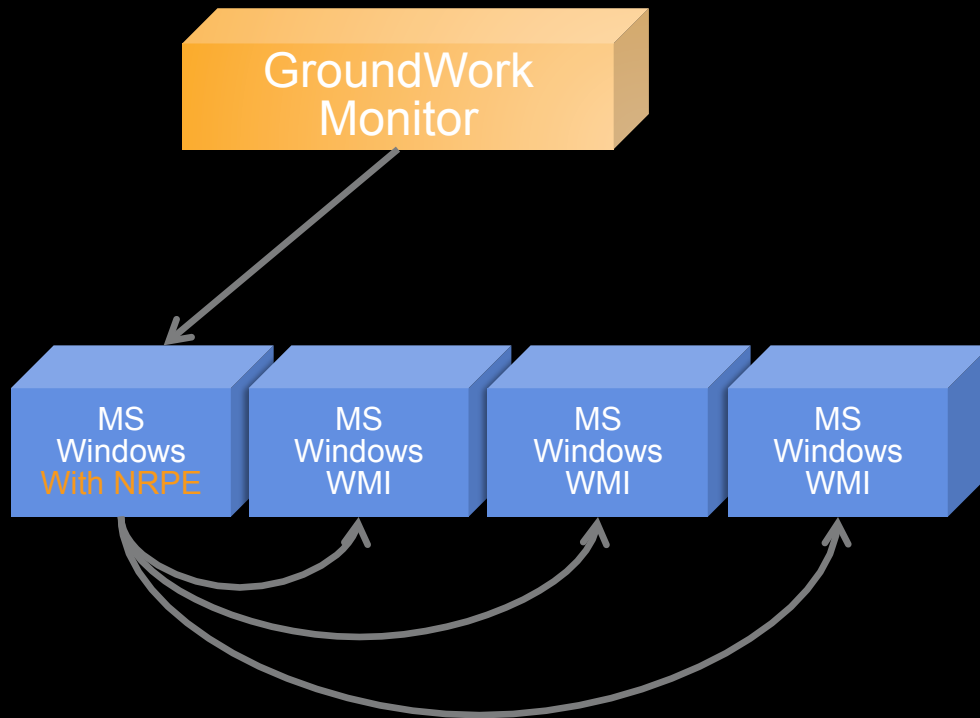
```
cscript.exe //nologo check_counter_counter.vbs -h localhost -class  
"Win32_PerfRawData_PerfOS_Memory" -inst "*" -prop "PagesPerSec"
```

```
OK - 'PagesPerSec' = 2.22133456;
```

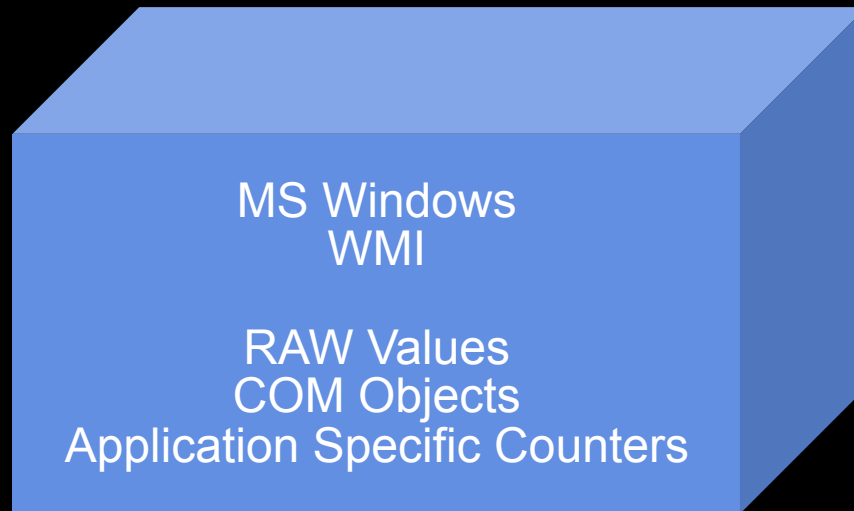
```
cscript.exe //nologo check_raw_fraction.vbs -h localhost -class  
Win32_PerfRawData_PerfDisk_LogicalDisk -inst Name=C: -prop  
PercentFreeSpace
```

```
OK - C: 'PercentFreeSpace' = 67;
```

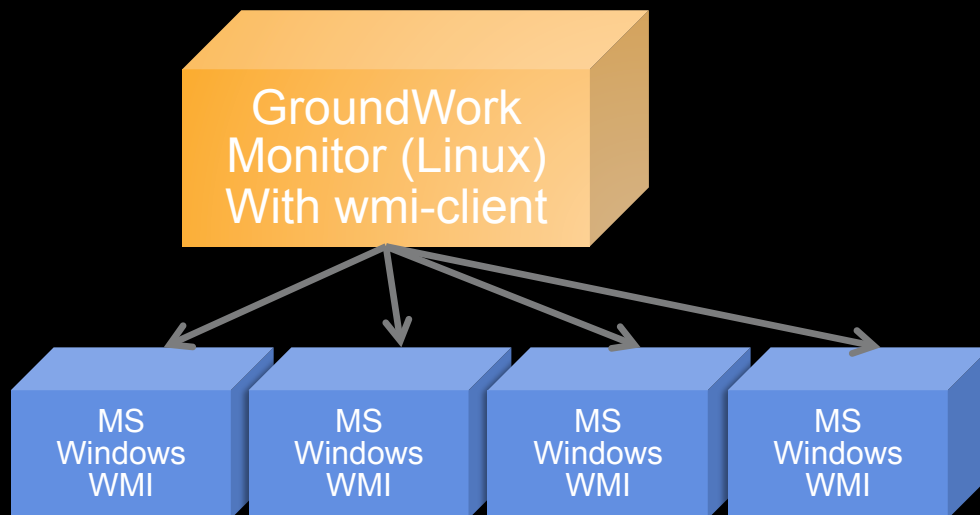
Windows Monitoring with WMI



Windows Monitoring with WMI

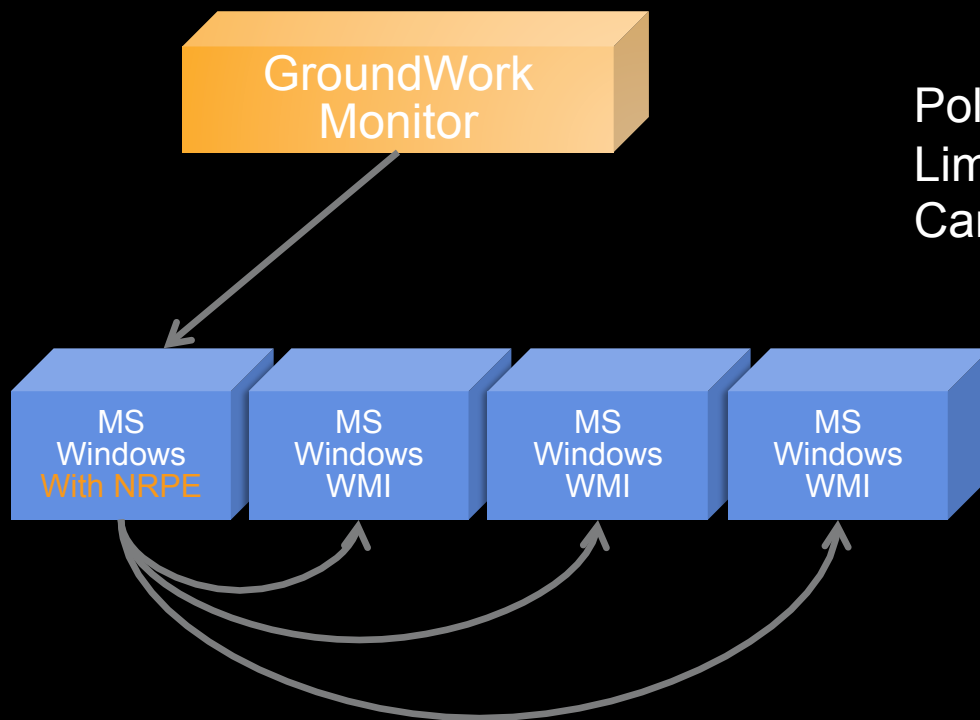


Windows Monitoring with WMI Direct from the GroundWork Server



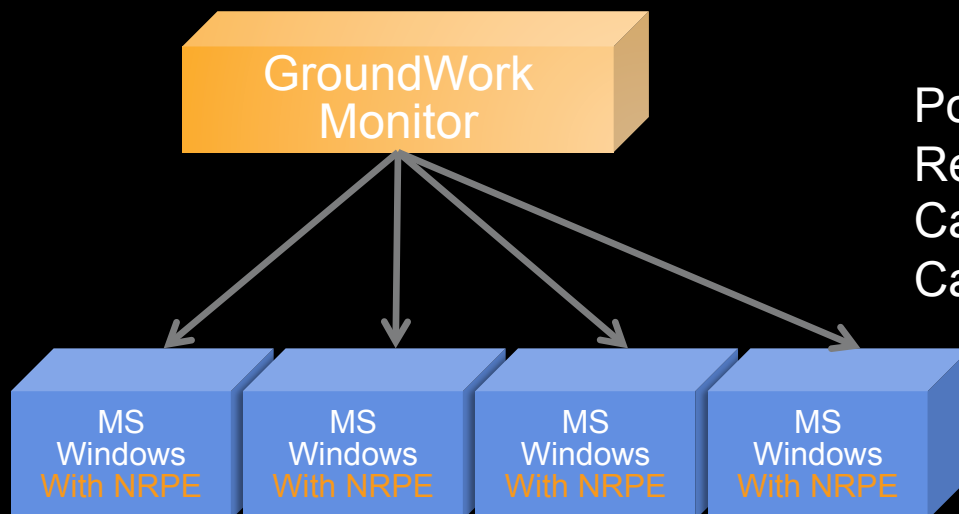
Slow...
Limited to WMI Counters...

Windows Monitoring with WMI With NRPE_NT as a Proxy



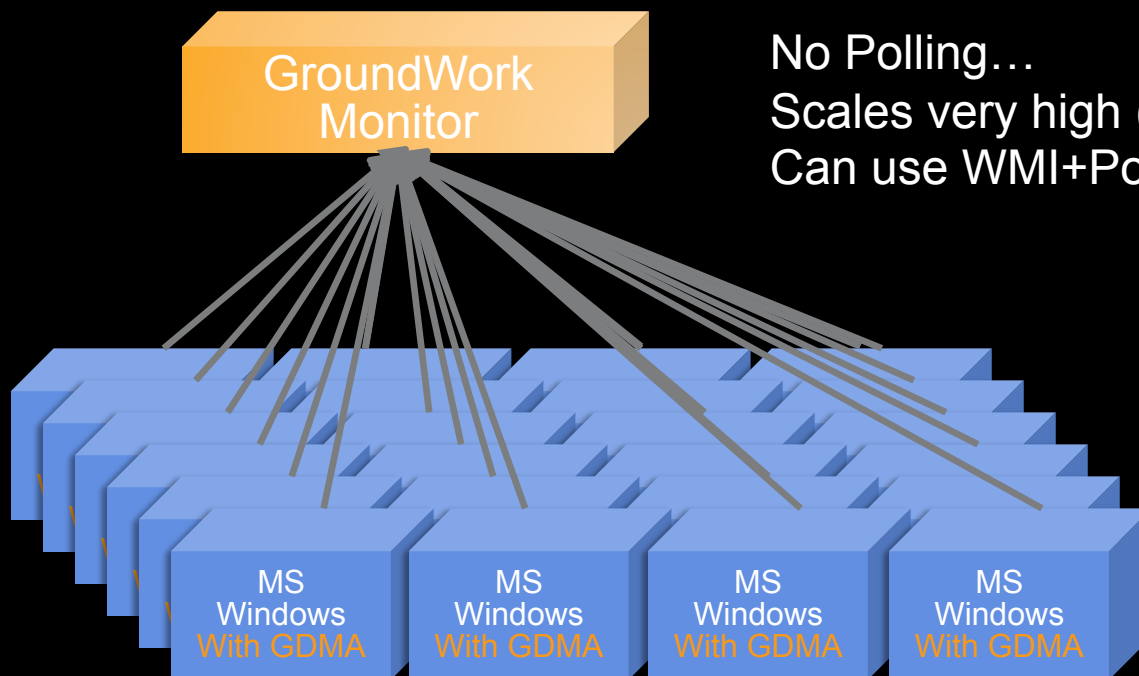
Polling Overhead...
Limited to around 100 hosts...
Can use WMI+Powershell...

Windows Monitoring with WMI and NRPE_NT Directly



Polling Overhead...
Requires Agents everywhere...
Can use WMI+Powershell...
Can use Event Handlers...

Windows Monitoring with Windows GDMA

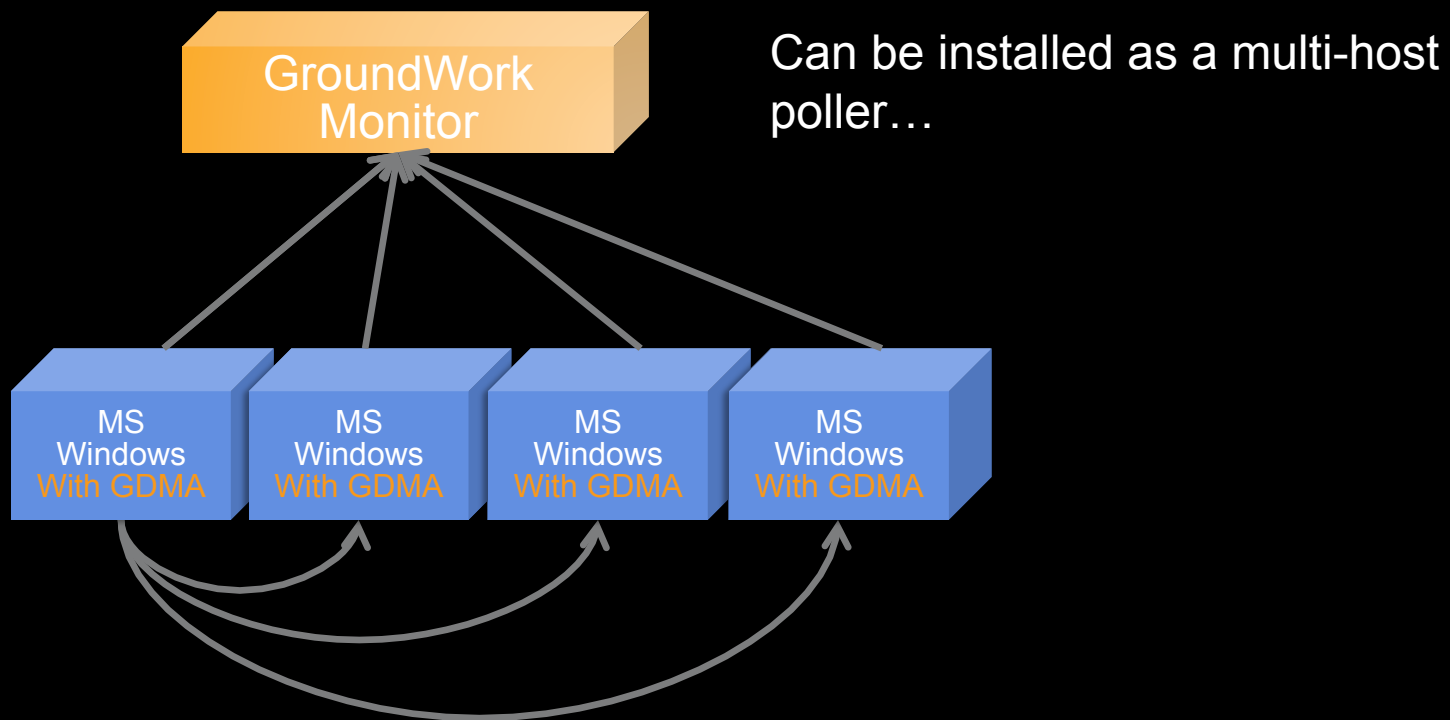


No Polling...

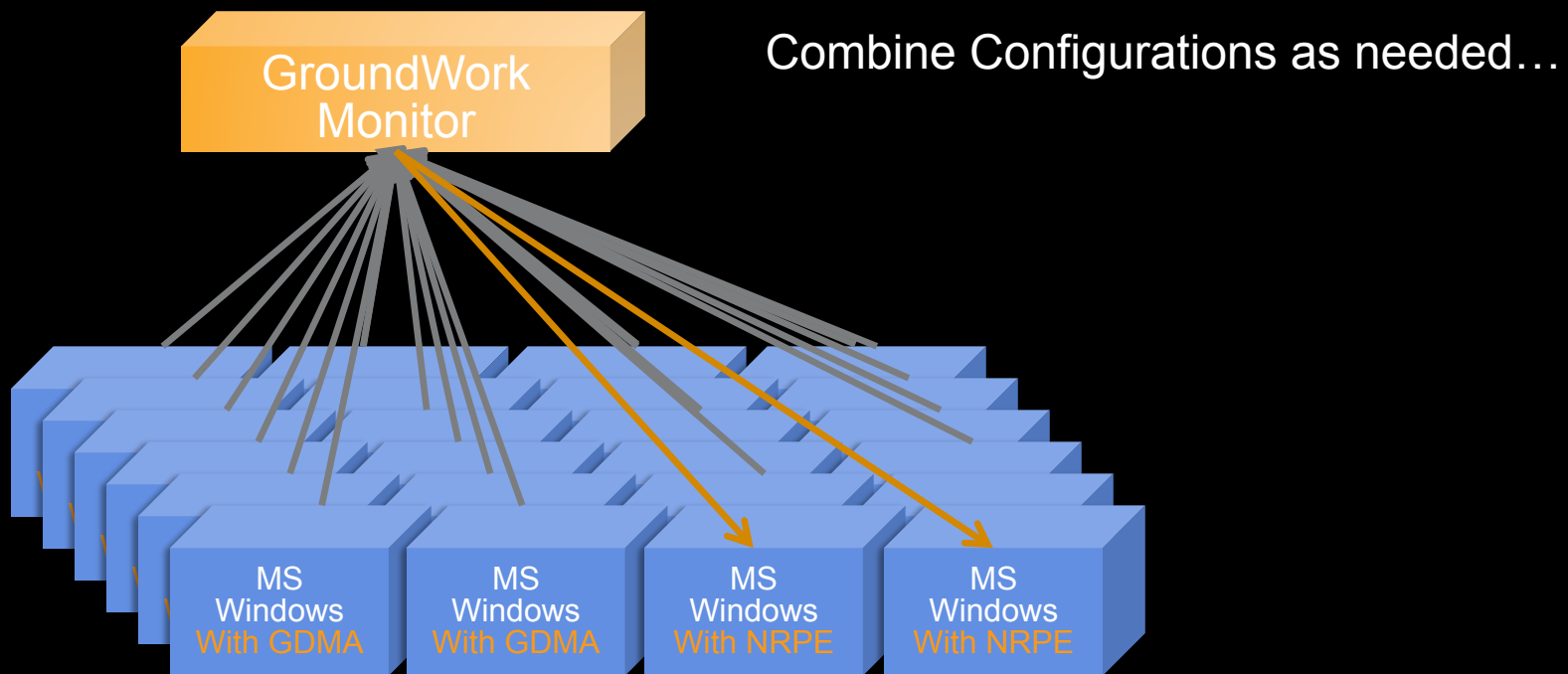
Scales very high (1000s of hosts)...

Can use WMI+Powershell...

Windows Monitoring with Windows GDMA



Windows Monitoring with Windows GDMA



In summary...

Lots of options...

- WMIC
- WMI Proxy
- NRPE_NT
- GDMA

Growing list of plugins in open source...

Your contributions welcomed!

Email support@gwos.com

Thanks for Listening!

Downloads...

MS Powershell:

<http://support.microsoft.com/kb/968929>

WMI Plugins:

<https://kb.groundworkopensource.com/display/SUPPORT/How+to+use+WMI+agentless+plugins>

GDMA:

<https://kb.groundworkopensource.com/display/FLEX/GroundWork+Distributed+Monitoring+Agent>