Monitoramento POWERSHELL

Prof: Paulo Maciel prmm@cin.ufpe.br

Instrutor: Jamilson Dantas jrd@cin.ufpe.br

Agenda

- Sobre o PowerShell
  - Calculadora
  - Comandos externos
- Instalação
- Comandos PowerShell
- Criando um Script
  - Executando

Sobre o PowerShell

- Nova geração de Shell (Família Microsoft Windows)
- Permite a execução remota (Versão 2.0)
- Integra com .NET Fremework

Sobre o PowerShell

- Calculadora

  5 – 4

  (5 + 9) * 4

  5GB/120MB

Sobre o PowerShell

- Comandos Externos

  – O PowerShell pode executar comandos do prompt de comandos Microsoft;

  ipconfig

  ls

  dir

Instalação

- Windows installer 3.1;
- .Net Fremework 2.0 SP 1;
- Powershell 1.0 (ou 2.0)

Comandos PowerShell

- Os comandos do powershell são chamados de cmdlets. Os nomes dos comandos são compostos por um verbo seguido de – e uma ação.

  – Digite no terminal:

    Get-Command

Criando um Script

- Criar um arquivo texto simples na raiz com o nome qualquer (ex: test.ps1) e edite o script abaixo:

  – “Massa d+”

Criando um Script

- Para executar:
  - Dar permissão

  Set-ExecutionPolicy RemoteSigned

  Executar

  .\test.ps1

Monitorando Processos

Get-Process

- Handles: o número de manipulações abertas pelo processo.
- NPM(K): a quantidade de memória não paginada usada pelo processo, em kilobytes.
- PM(K): a quantidade de memória paginada usada pelo processo, em kilobytes.
- WS(K): o tamanho do conjunto de trabalho do processo, em kilobytes. O conjunto de trabalho consiste nas páginas de memória recentemente referenciadas pelo processo.
- VM(M): a quantidade de memória virtual usada pelo processo, em megabytes. A memória virtual inclui o armazenamento em disco dos arquivos de paginação.
- CPU(s): o tempo do processador que o processo usou em todos os processadores, em segundos.
- ID: a ID de processo (PID) do processo.
- ProcessName: o nome do processo.

Monitorando Processos

```
get-process | where-object {$_.WorkingSet -gt 20000000}

Get-Counter '\Memory\Available MBytes‘

Get-Counter '\Processor(_Total)\% Processor Time‘

Get-Counter "\Processo(firefox)\% tempo de processador"
```