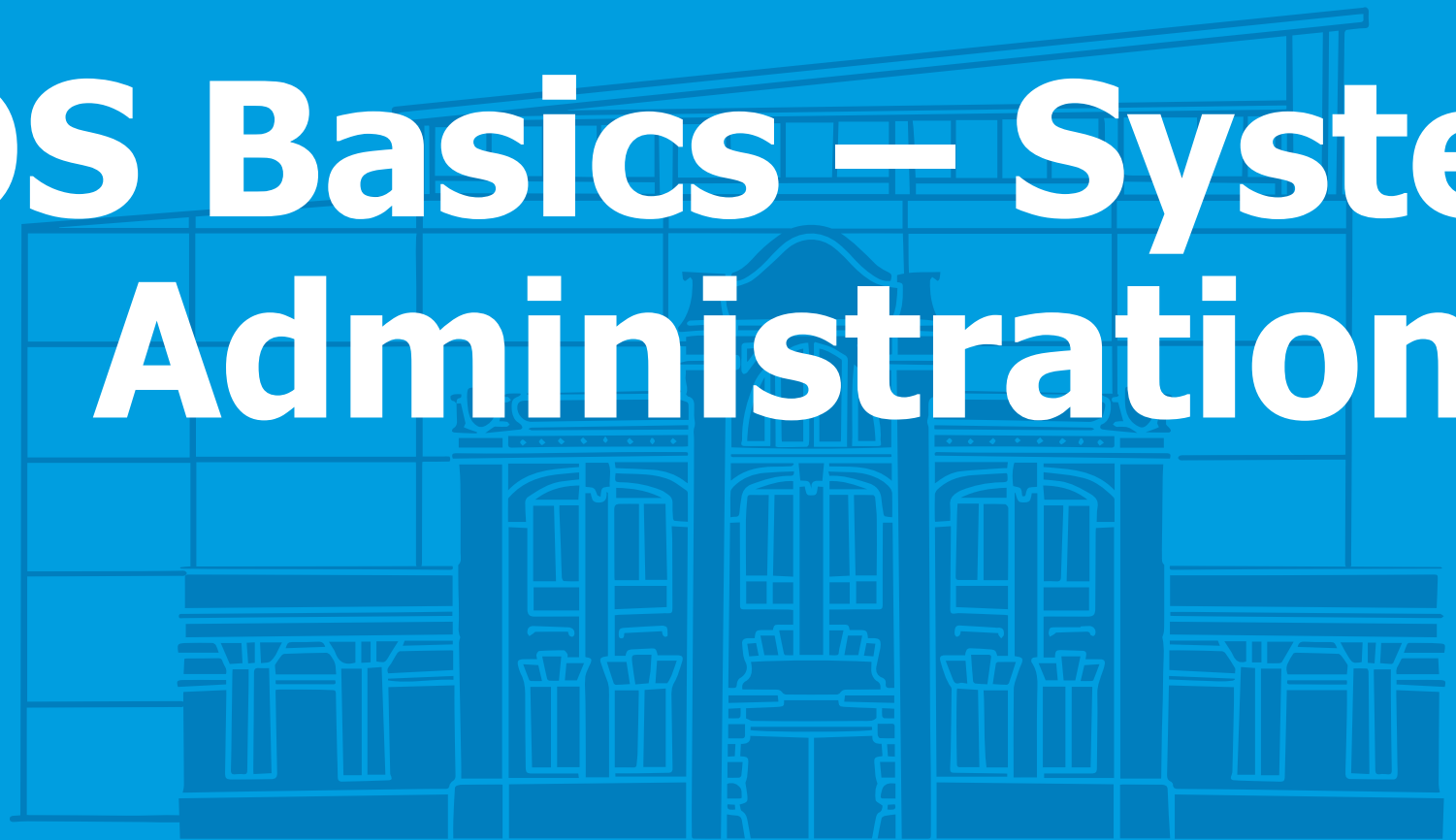
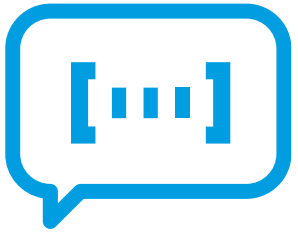
netmind
a bts company

MI1762

OS Basics – System Administration



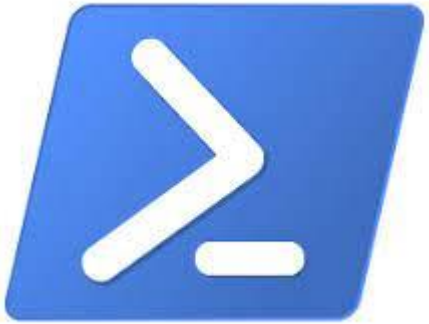


Windows system administration

02

PowerShell

- Windows PowerShell is an **object-oriented automation engine** and **scripting language**.
- It is designed mainly for IT professionals and system administrators to **control & automate the administration of Windows OS** and other applications.
- It **combines the flexibility of scripting, command-line speed, and the power of a GUI-based admin tool**.
- It allows to **solve problems efficiently** by helping system admin to eliminate future manual labor hours.



OBJECTIVE

Review Windows PowerShell commands

INSTRUCTIONS

1. PowerShell commands are known as **cmdlets**, and these cmdlets are the driving force behind its functional capabilities.
2. From commands that improve the overall Windows experience to commands useful for development work, **there are dozens of important commands** we should know.
3. We are going to **explore** some of those **commands and its use**.
4. The general reference can be reviewed here:

   https://docs.microsoft.com/es-es/powershell/module/activedirectory/?view=windowsserver2022-ps

90 min

Basic commands

Basic	
Commands list	get-command
Quick access to the information	Get-Help [[-Name] <String>] [-Path <String>] [-Category <String[]>] [-Component <String[]>] [-Functionality <String[]>] [-Role <String[]>] [-Examples] [<CommonParameters>]
Performs an operation against every item in a specified group of input objects.	Get-Process | ForEach-Object {Write-Host $_.name -foregroundcolor cyan}
Set an alias for a cmdlet	Set-Alias New-Alias np c:\windows\system32\notepad.exe

Basic commands

Basic Configuration	
Control the level of security surrounding PowerShell scripts.	Get-ExecutionPolicy
Services information	Get-Service
Machine's event logs	Get-EventLog -Log "Application"
List of all the currently running processes	Get-Process
Stop processes	Stop-Process -processname [name]
Add / Clear to session history	Add-History Clear-History -Command *help*, *command
Take a dataset and pass it further down your pipeline for filtering	Where-Object Get-Service | Where-Object {$_.Status -eq 'Running'}
Add an Authenticode signature to a script or file.	Set-AuthenticodeSignature
Set a restore point on your machine	Checkpoint-Computer -Description "My 2nd checkpoint" -RestorePointType "Modify_Settings"

System Diagnostics

Check Current Memory Usage	Get-WmiObject WIN32_PROCESS | Sort-Object -Property ws -Descending | Select-Object -first 10 ProcessID,Name,WS
Process Monitoring	$ProcessName = '[processname]' Get-Process -Name $ProcessName Out-File -FilePath C:\Windows\Logs\Report.csv
Monitor Processes, Memory, and CPU Usage	Get-Counter '\Memory\Available MBytes' Get-Counter '\Processor(_Total)\% Processor Time'
Virtual Memory Statistics	Get-Ciminstance Win32_OperatingSystem Get-Process gps gps | sort vm | ? vm -gt 1000Mb | fw name
Process and Services Monitoring	Get-Service -Name RasMan | Select-Object -Property *

System Diagnostics

Debug a process	Debug-Process
Get performance data from local or remote computers	Get-Counter Get-Counter -Counter "\Processor(_Total)\% Processor Time" -SampleInterval 2 -MaxSamples 3
Exports PerformanceCounterSampleSet objects as counter log files.	Export-Counter Get-Counter "\Processor(*)\% Processor Time" | Export-Counter -Path C:\Temp\PerfData.blg
Verify whether items exist in a specified path	Test-Path C:\Scripts\Archive
Windows event logs	Get-WinEvent
Troubleshooting packs are collections of PowerShell scripts and assemblies that help you troubleshoot, diagnose, and repair common system problems	Invoke-TroubleshootingPack
Measuring how long a script or scriptblock to run.	Measure-Command { Mount-SPContentDatabase –Name wss_content_portal –WebApplication http://portal.contoso.com }
Know how large a given object is.	Measure-Object

System Diagnostics

Work with events	Register-EngineEvent Register-ObjectEvent Remove-Event
Suspend the activity in a script or session	Start-Sleep -Seconds xxx
Analyzing performance or code quality	Tee-Object [-FilePath] <string> [-InputObject <psobject>] [<CommonParameters>]
Evaluating whether input files are permitted to run for a specific user based on the specified AppLocker policy.	Test-AppLockerPolicy [-PolicyObject] -Path [-User] [-Filter >] []
Tests and repairs the connection between a local computer and its domain.	Test-ComputerSecureChannel –credential WINDOWSITPRO\Administrator –Repair
Determining whether all elements of a path exist.	test-path z:\foo
Configuring and starting the trace of a specified command or expression.	Get-TraceSource -Name *param*

Network Diagnostics

The ping Command	ping google.com ping 216.58.217.110
The Test-NetConnection Command	Test-NetConnection www.google.com
Network Packet Analyzer	(gcm -Module NetEventPacketCapture | measure).count
Network Statistics	netsh interface ipv4 show ipstats NetStat Get-NetAdapterStatistics
Performance counters	Get-Counter -ListSet * | Sort-Object CounterSetName | Select-Object CounterSetName

File System Management

Set a restore point on your machine	Checkpoint-Computer -Description "My 2nd checkpoint" -RestorePointType "Modify_Settings"
Upload Files to a Remote Server	$b = New-PSSession B Copy-Item -FromSession $b C:\Programs\temp\test.txt -Destination C:\Programs\temp\test.txt
Symbolic Links/Hard links	New-Item -ItemType SymbolicLink -Path "Link" -Target "Target" New-Item -ItemType HardLink -Path "Link" -Target "Target"
Monitor Disk I/O	Get-Counter -ListSet "*disk*" | Select CounterSetName Get-Counter -ListSet LogicalDisk | Select -ExpandProperty Counter
Listing All the Files and Folders Within a Folder	Get-ChildItem -Path C:\ -Force
Copying Files and Folders	Copy-Item Copy-Item -Filter *.txt -Path c:\data -Recurse -Destination C:\temp\text
List Open Files	Get-SmbOpenFile
Creating Files and Folders	New-Item -Path 'C:\temp\New Folder' -ItemType Directory

File System Management

Removing All Files and Folders Within a Folder	Remove-Item -Path C:\temp\DeleteMe
Mapping a Local Folder as a drive	New-PSDrive -Name P -Root $env:ProgramFiles -PSProvider FileSystem

Package Management

https://docs.microsoft.com/en-us/powershell/module/packagemanagement/?view=powershell-7.2

Finds software packages in available package sources.	Find-Package
Returns a list of Package Management package providers available for installation.	Find-PackageProvider
Returns a list of all software packages that were installed with **PackageManagement**.	Get-Package
Returns a list of package providers that are connected to Package Management.	Get-PackageProvider
Gets a list of package sources that are registered for a package provider.	Get-PackageSource
Adds Package Management package providers to the current session.	Import-PackageProvider
Installs one or more software packages.	Install-Package
Installs one or more Package Management package providers.	Install-PackageProvider
Adds a package source for a specified package provider.	Register-PackageSource
Saves packages to the local computer without installing them.	Save-Package
Replaces a package source for a specified package provider.	Set-PackageSource
Uninstalls one or more software packages.	Uninstall-Package
Removes a registered package source.	Unregister-PackageSource

Text Manipulation

Delete the contents of an item but retain the item itself	Clear-Content C:\Temp\TestFile.txt Clear-Content -path * -filter *.TXT –force
Search a string in multiple files	Get-ChildItem -Recurse | Select-String "dummy" -List | Select Path
Find and Replace in multiple files	Get-ChildItem -Recurse | ForEach { (Get-Content $_.PSPath \| ForEach {$ -creplace "old", "new"}) | Set-Content $_.PSPath }
Reading a Text File into an Array	Get-Content -Path C:\boot.ini

For text manipulation in script mode:

https://docs.microsoft.com/en-us/powershell/scripting/learn/deep-dives/everything-about-string-substitutions?view=powershell-7.2

Managing Files

Compress or decompress	Compress-Archive Expand-Archive
View/Set your current directory	Get-Location Set-Location
View all items within your current working directory	Get-ChildItem
Change file permissions	CACLS myfile.txt /E /G "Power Users":R Get-Acl -Path "C:\Dog.txt" | Set-Acl -Path "C:\Cat.txt"

PoweShell scripting

- PowerShell can save you a lot of time on Windows **admin tasks**.
- Powershell scripts can **include any windows command** and are store in **.ps1** file.
- By default, you can’t run a script by just double-clicking a file. This protects your system from accidental harm.

PoweShell scripting

- For calling a script must use:
  & "<path_to_script>/Script_Name.ps1“

- **For example.**
  - Write next line :

  Write-Host get-date

  - In file: *GetDate.ps1* right in c:\.
  - To execute:

  & "C:\GetDate.ps1"

OBJECTIVE

Creating a Powershell script

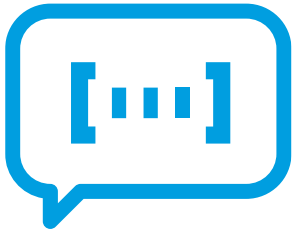
INSTRUCTIONS

1. **Follow the next tutorial** on creating a monitor script:
   https://www.techtarget.com/searchitoperations/tutorial/Build-a-PowerShell-performance-monitoring-script-step-by-step

2. **Execute** the script.

20 min

netmind
a bts company



Linux system administration

03

OBJECTIVE

Review Linux commands

INSTRUCTIONS

1. There are **tons of linux commands** for system administration.
2. In next slides you will find **some usual and useful command in Linux**.
3. We are going to **explore** some of those **commands and its use**.

90 min

Basic commands

Basic	
Command manual	man [command name]
Run programs with the security privileges	sudo [command]

Basic Configuration	
Set the Hostname	hostname hostname -f
Set the Time Zone	dpkg-reconfigure tzdata
Set the Time Zone Manually	ln -sf /usr/share/zoneinfo/UTC /etc/localtime
Configure the /etc/hosts File	vi /etc/hosts File

System Diagnostics

Check Current Memory Usage	free -m
Monitor I/O Usage with vmstat	vmstat 1 20
Linux Process Monitoring	top
Monitor Processes, Memory, and CPU Usage with htop	htop
Virtual Memory Statistics	vmstat
Monitor User Activity	psacct or acct
Linux Process and Services Monitoring	monit
System and Network Monitoring	monitorix
Monitor Linux Performance	Nmon
All-in-One Performance Monitoring Tool	Collectl

Network Diagnostics

The ping Command	ping google.com ping 216.58.217.110
The traceroute Command	traceroute www.google.com
The mtr Command	mtr www.google.com mtr --report
Network Packet Analyzer	tcpdump -i enp0s3
Network Statistics	netstat -a | more
Real-Time IP LAN Monitoring	sudo apt install iptraf iptraf
Monitor Per Process Network Bandwidth	nethogs
Network Bandwidth Monitoring	iftop
Ethernet Activity Monitor	arpwatch
Network Security Monitoring	suricata
Monitoring Network Bandwidth	vnstat
Network/Server Monitoring	nagios

File System Management

Upload Files to a Remote Server	scp [/path/to/local/file] [remote-username]@[remote-hostname]:[/path/to/remote/file]
Symbolic Links	ln -s [/path/to/target/file] [/path/to/location/of/sym/link]
Manage Files on a Linux System	**copy:** cp /home/username/todo.txt /home/username/archive/todo.01.txt cp -R /home/username/archive/ /srv/backup/username.01/ **move:** mv /home/username/archive/ /srv/backup/username.02/ **delete:** rm scratch.txt
List Open Files	Lsof
Monitor Linux Disk I/O	Iotop
Input/Output Statistics	Iostat

Package Management

https://ubuntu.com/server/docs/package-management

Upgrade packages	sudo apt upgrade
Install/remove package	sudo apt install nmap sudo apt remove nmap
Find Packages Installed on Your System	dpkg -l
Find Package Names and Information	apt-cache search [package-name] apt-cache show [package-name]

Text Manipulation

Search for a String in Files with grep	grep "^Subject:.*HELP.*" /home/username/mbox grep -i "morris" ~/org/*.txt ls /home/username/data | grep "1257"
Search and Replace Across a Group of Files	sed -i `s/^good/BAD/` morning-star.txt
Edit Text	nano /etc/hosts vi /etc/hosts emacs /etc/hosts zile /etc/hosts
Show Logs	tail -F /var/log/apache2/error.log tail -F /var/www/html/example.com/logs/error.log

Managing Files in Linux

compress or decompress	gzip, xz, and bzip2
View your current directory	echo $PWD pwd
View all items within your current working directory	ls ls -alh
Change file permissions	chmod chmod [OPTIONS] [ugoa…][-+=]perms…[,…] FILE…

Shell scripting

A shell script is a **computer program designed to be run by the Unix/Linux shell** which could be one of the following:

In Linux There are different shells, but the ones we should care about are:

- Bourne shell (sh),
- Bourne Again shell (bash),
- Z shell (zsh)

OBJECTIVE

Examining a script

INSTRUCTIONS

1. Open the **writename.sh** script and read the code.
2. **Execute** the script.
3. You can **read more** about shell scripting in next link:
   https://github.com/syndbg/shell-in-a-nutshell/blob/master/GUIDE.md

15 min

EXERCISE

Server administration cheat sheet

OBJECTIVE

Generate a cheat sheet about server administration!

INSTRUCTIONS

Step 1: Create an infographics about server administration.

- **Be very artistic!**
- Find inspiration in the Internet.

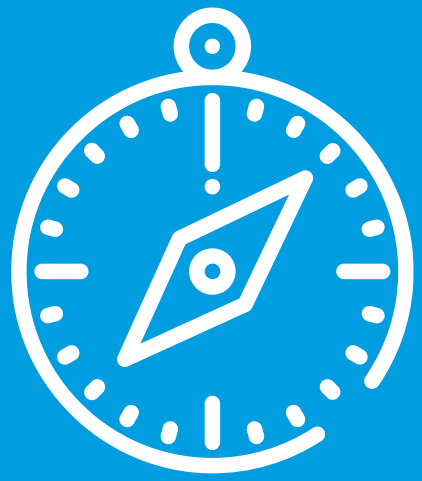
Step 2: Enter the contest and send your artwork to the trainer.

Step 3: Participants will:

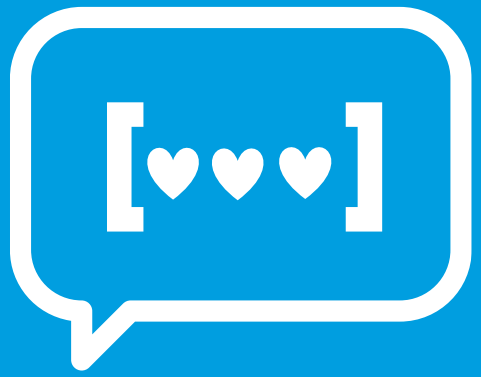
- Explain their creation.
- Will be voted by the class.

Step 5: The responder with the higher score wins!

40 min



Next steps



We would like to know your opinion!

Please, let us know what you think about the content.
From Netmind we want to say thank you, we appreciate time and effort you have taking in answering all of that is important in order to improve our training plans so that you will always be satisfied with having chosen us
quality@netmind.es

netmind
a bts company

Thanks!

Follow us:

netmind
a bts company

EMPOWERING DIGITAL TEAMS

netmind.net

Barcelona

C. dels Almogàvers 123
08018 Barcelona
Tel. +34 933 041 720
Fax. +34 933 041 722

Madrid

C. Bambú, 8
28036 Madrid
Tel. +34 914 427 703
Fax +34 914 427 707

Atlanta

3372 Peachtree Road NE
Suite 115
T. +1 (678) 366 1393
Atlanta, GA 30326