PowerShell Core Install and Logging

PowerShell Core, the cross-platform version of PowerShell, is free to install and use. Detailed instructions for installing PowerShell Core on Windows, Linux and macOS are found [here](https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell). On Windows, we can simply install it with the following command:

winget install --id Microsoft.PowerShell

Text

Description automatically generated

Install PowerShell Core on your lab VM and then run it by searching for **pwsh** in the start menu.

Graphical user interface, application

Description automatically generated

Notice how it has a black icon by default which helps us distinguish it from the built-in **Windows PowerShell.**

Graphical user interface, application

Description automatically generated

In the image above I’ve got PowerShell Core and Windows PowerShell executing commands side by side. There are no issues with running both versions of PowerShell on the same system at the same time. There really isn’t anything new to say about the way you use PowerShell from PowerShell Core vs. Windows PowerShell because the usage is essentially the same.

However, when it comes to logging, there are different ways to control the log settings and the logs are in a different location. You can find the PowerShell Core logs in the **“Applications and Services Logs”🡪PowerShellCore🡪Operational** Log. On Linux, you’ll find the logs in syslog and on macOS you’ll find them in the **os\_log**.

Graphical user interface, application

Description automatically generated

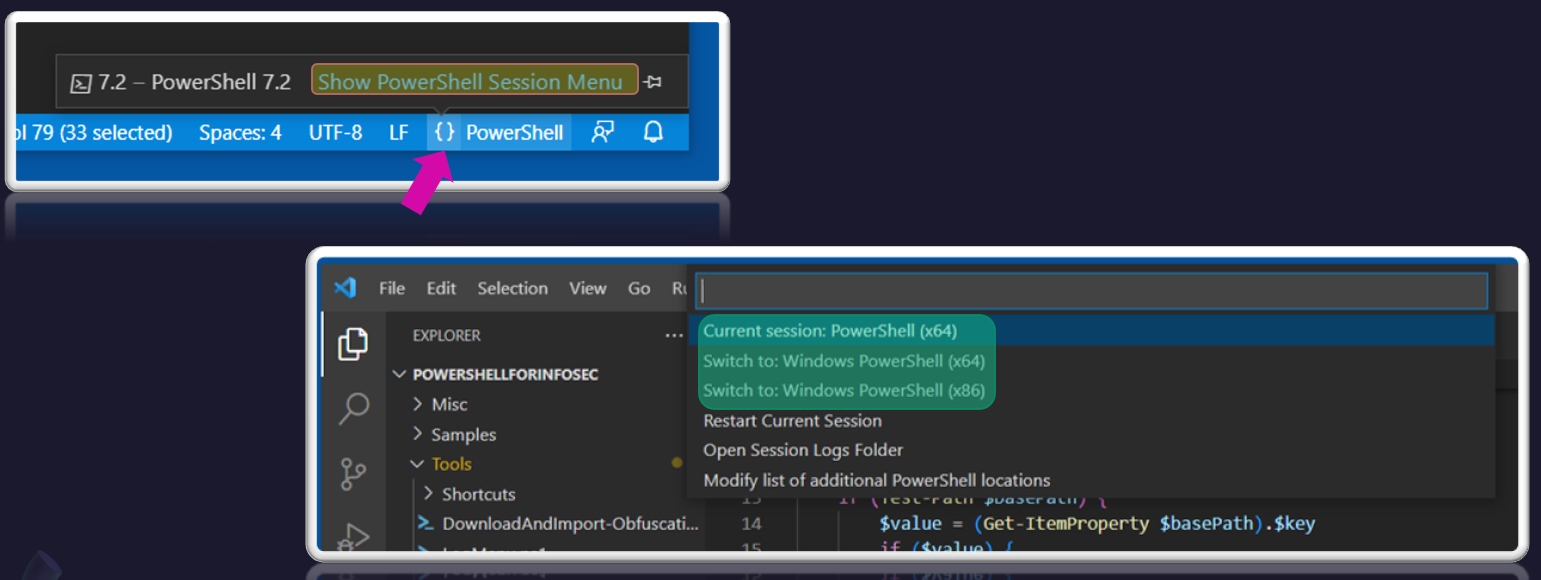
You will need to use the **PWSH (Core) log** tail application instead of the **TailPSopLog** if you want to see the color coded, automatically updating version of this log as you play with PowerShell Core.

Text

Description automatically generated

The **LogMenu** tool that you used in the Windows PowerShell logging lab, also works to set the PowerShell Core Logging options. It does this by using the **UseWindowsPowerShellPolicySetting** registry key, instructing PowerShell Core to use the same log settings as Windows PowerShell.

Remember if you are using Visual Studio Code to assist you with creating your PowerShell scripts, you can use the PowerShell Session Menu to select which version of PowerShell you want it to use.



The good news is, that there aren’t many differences that affect how we use PowerShell that we need to be concerned with between Core and Windows PowerShell so we can still apply all of our learning from this class to PowerShell Core as well.

Do you have a Linux or macOS test system you can install PowerShell Core on? Give it a try!

You will notice some differences between PowerShell Core on Windows vs Linux and Mac. Windows is the only Operating System where you will find AMSI integration and configurable execution policies. Another major difference is which protocol is used for executing remote commands (PowerShell Remoting). When Linux or macOS operating systems are involved, PowerShell remoting is accomplished through the SSH Protocol and extra setup steps must be taken as follows.

Table

Description automatically generated

It is exciting to see PowerShell accessible cross-platform and to be able to use a single skillset to manage multiple operating systems.