Getting Started with PowerShell Scripting

UNDERSTANDING POWERSHELL SECURITY

Liam Cleary

CEO / MICROSOFT MVP / MICROSOFT CERTIFIED TRAINER

@shareplicity www.shareplicity.com | @helloitsliam www.helloitsliam.com

Overview

Review PowerShell Execution Policies

Review Execution Policy Precedence

Understanding PowerShell Scopes

Setting Execution Policies

What are PowerShell Execution Policies?

What are PowerShell Execution Policies?

Safety feature to control the conditions a script can run

Prevent execution of malicious scripts

Scope execution of scripts to specific sessions

What are PowerShell Execution Policies?

Execution policies for the local computer and current user are stored in the registry

The execution policy isn't a security system that restricts user actions

On a Windows computer you can set an execution policy for the local computer, for the current user, or for a particular session

On non-Windows computers, the default execution policy is Unrestricted and cannot be changed

Enforcement of policies only occurs on Windows platforms

PowerShell Execution Policies

- All Signed
- Bypass
- Remote Signed
- Restricted
- Unrestricted

All Signed Policy

Scripts can execute

Requires that all scripts and configuration files be signed by a trusted publisher

Prompts you before running scripts not yet classified as trusted or untrusted

Risk running signed malicious scripts

Bypass Policy

Nothing is blocked and there are no warnings or prompts

This execution policy is designed for configurations in which a PowerShell script is the foundation for a program that has its own security model

Remote Signed Policy

Scripts can execute

Requires a digital signature from a trusted publisher

Doesn't require digital signatures on scripts that are written locally

Run scripts that are not signed, if the scripts are unblocked

Risk running unsigned scripts and signed scripts that could be malicious

Restricted Policy

The default execution policy for Windows client computers

Permits individual commands but does not allow scripts

Prevents running of all script files

Unrestricted Policy

The default execution policy for non-Windows computers

Unsigned scripts can execute

Risk of running malicious scripts.

Warns the user before running scripts and configuration files that are not from the local intranet zone

Understanding PowerShell Scopes

Understanding PowerShell Scopes

Execution Policies can be set at **CurrentUser** and **LocalMachine** levels which are then stored in the registry

Process

Affects only the current PowerShell session

Current User

Policy affects only the current user

Local Machine

Affects all users on the current computer

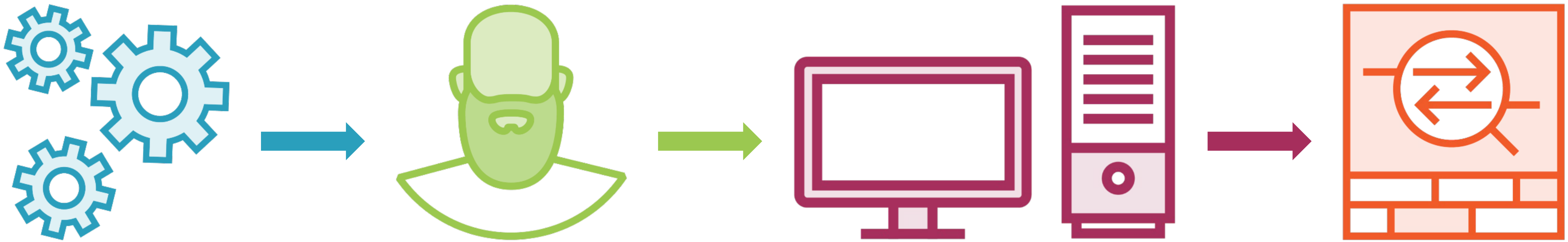
Group Policy Based Scopes

Machine Policy
Set by a Group Policy for all users of the computer

User Policy
Set by a Group Policy for the current user of the computer

Review Execution Policy Precedence

Execution Policy Precedence



Process

Current User

Local Machine

Restricted

Retrieve Execution Policy Precedence

```
# Retrieve all the execution policies and display them in precedence order
Get-ExecutionPolicy -List
```

Demo

Review PowerShell execution policy precedence

Setting Execution Policies

Setting Execution Policies

Can be assigned to the default scope or a specific scope

The default scope is **LocalMachine**, which affects everyone who uses the computer

Execution policies can be used for a single PowerShell Session

Set the Default Execution Policy

```
# Retrieve the current execution policy
Get-ExecutionPolicy

# Set the current execution policy to Unrestricted
Set-ExecutionPolicy Unrestricted
```

Set a Scoped Execution Policy

```
# Set an execution policy for the LocalMachine scope
Set-ExecutionPolicy `
    -ExecutionPolicy RemoteSigned `
    -Scope LocalMachine

# Set an execution policy for the CurrentUser scope
Set-ExecutionPolicy `
    -ExecutionPolicy AllSigned `
    -Scope CurrentUser

# Set the execution policy from a remote computer to a local computer
Invoke-Command `
    -ComputerName Computer `
    -ScriptBlock { Get-ExecutionPolicy } | Set-ExecutionPolicy
```

Set Execution Policy for Single Session

Launch PowerShell using command Line

- `pwsh.exe`

Utilize execution policy parameter

- `ExecutionPolicy AllSigned`

Does not save to the registry

Demo

Retrieve the current execution policy

Set the default execution policy

Set a scoped execution policy

Launch a PowerShell session with execution policy

Summary

Reviewed PowerShell Execution Policies

Reviewed Execution Policy Precedence

Understood the Purpose of PowerShell Scopes

Set Execution Policies

Up Next:
Controlling the flow of PowerShell Functions