

Powershell

Verb-Noun	Structure
Verb-N...	Tab for intellisense
Stop-Service <inputObject>	Parameters are required

Example:

```
Get-Eventlog -LogName System -Newest 5 | Format-List Out-File c:\log.txt
```

Remote Access via Powershell

winrm quickconfig	brings the service on
Get-Process -ComputerName SVR	
Stop-Process	
Get-Service -ComputerName SVR	
Invoke-Command -ComputerName SVR -ScriptBlock {get-eventlog -LogName Security -Newest 5}	
Enter-PSSession -ComputerName SVR	
Exit	
Get-Process -ComputerName SVR,DC (runs on both)	

CredSSP

Scenario:

1. Logged into ServerA, remote powershell to ServerB
2. ServerB powershell command attempts to access ServerC
3. Access is denied because credentials not passed from ServerB to ServerC

Credential Security Support Provider (CredSSP)

- CredSSP caches credentials on the remote server (ServerB)
- Opens up credential theft attacks if the remote server is compromised
- Disabled by default, only enable this in trusted environments

Integrated Scripting Environment (ISE)

Get-Variable	
\$Number1 = 5	Stores the value in a new variable
\$Number	outputs 5
\$Name = "SVR"	Can now use -ComputerName \$Name
ISE	opens integrated scripting environment (click show script pane)
\$name = Read-Host "Which computer would you like to connect to?"	
\$log = Read-Host "Which log would you like to see?"	
\$amount = Read-Host "How many of the newest entries would you like to see?"	
Get-Eventlog -ComputerName \$name -LogName \$log -Newest \$amount	

Revision #4
Created 2026-07-16 02:40:25 UTC by Admin
Updated 2026-07-19 22:57:59 UTC by Admin