Windows Server Core PowerShell Cheat Sheet

```
############################################################
# Windows Server Core Setup & Configuration Script
# Author: Edy Werder
# Description: Categorized PowerShell commands for common tasks
############################################################

# === [INITIAL CONFIGURATION] ===
Rename-Computer -NewName "SERVER01" -Restart
New-NetIPAddress -IPAddress "192.168.1.100" -PrefixLength 24 -DefaultGateway "192.168.1.1" -InterfaceIndex 12
Set-DnsClientServerAddress -InterfaceIndex 12 -ServerAddresses "192.168.1.10","192.168.1.11"
Add-Computer -DomainName "contoso.com" -Credential (Get-Credential) -Restart

# === [ROLE INSTALLATION] ===
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
$pass = Read-Host "Enter DSRM password" -AsSecureString
Install-ADDSForest -DomainName "contoso.com" -SafeModeAdministratorPassword $pass -InstallDns -Force
Install-WindowsFeature DNS -IncludeManagementTools
Install-WindowsFeature DHCP -IncludeManagementTools
Add-DhcpServerInDC -DnsName "server01.contoso.com" -IpAddress 192.168.1.100
Install-WindowsFeature Hyper-V -IncludeManagementTools -Restart
Install-WindowsFeature Web-Server -IncludeManagementTools
Install-WindowsFeature FS-FileServer
Install-WindowsFeature Storage-Services
Install-WindowsFeature FS-DFS-Namespace, FS-DFS-Replication
Install-WindowsFeature NET-Framework-Core -Source D:\sources\sxs
Install-WindowsFeature RSAT-AD-PowerShell

# === [FIREWALL HARDENING] ===
Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled True
Set-NetFirewallProfile -Profile Domain,Private,Public -DefaultInboundAction Block -DefaultOutboundAction Allow
New-NetFirewallRule -DisplayName "PowerShell Remoting" -Direction Inbound -Protocol TCP -LocalPort 5985,5986 -Action Allow -RemoteAddress "192.168.1.0/24"
New-NetFirewallRule -DisplayName "RDP Access" -Direction Inbound -Protocol TCP -LocalPort 3389 -Action Allow -RemoteAddress "192.168.1.0/24"
Get-NetFirewallRule | Where-Object {$_.Enabled -eq 'True'}

# === [WINRM & REMOTING DIAGNOSTICS] ===
Test-WSMan -ComputerName "server01.contoso.com"
Get-WSManCredSSP
Get-Item WSMan:\localhost\Client\TrustedHosts

# === [NETWORK DIAGNOSTICS] ===
Get-NetAdapter | Format-Table Name, Status, LinkSpeed
Test-NetConnection -ComputerName "dc01.contoso.com" -Port 389
Resolve-DnsName "contoso.com"
Get-NetIPAddress | Where-Object {$_.AddressFamily -eq "IPv4"}
Test-NetConnection -TraceRoute -ComputerName "8.8.8.8"

# === [PERFORMANCE MONITORING] ===
```

Windows Server Core PowerShell Cheat Sheet

```
Get-Counter "Processor(_Total)\% Processor Time" -SampleInterval 5 -MaxSamples 12
Get-Counter "\Memory\Available MBytes"
Get-Counter "\LogicalDisk(_Total)\% Disk Time"

# === [EVENT LOG FORWARDING] ===
wecutil qc /q
Set-Service -Name Wecsvc -StartupType Automatic
Start-Service Wecsvc

# === [SERVICE HARDENING] ===
Get-Service -Name "Themes","TabletInputService" -ErrorAction SilentlyContinue | ForEach-Object {
Set-Service -Name $_.Name -StartupType Disabled }

# === [WINDOWS UPDATE TROUBLESHOOTING] ===
sc query wuauserv
net stop wuauserv
net stop cryptSvc
net stop bits
net stop msiserver
Remove-Item -Recurse -Force C:\Windows\SoftwareDistribution
Remove-Item -Recurse -Force C:\Windows\System32\catroot2
net start wuauserv
net start cryptSvc
net start bits
net start msiserver

# === [FIREWALL VERIFICATION] ===
Get-NetFirewallRule -DisplayName "*Remote*" | Format-Table DisplayName, Enabled, Direction
netstat -an | findstr :5985
netstat -an | findstr :5986
```