Recovery

The *Diskpart.exe* command utility can be used to manage hard drives and volumes on the local machine.

To get help with a specific command type the command with /?. For example, to get help with the 'list' Diskpart command type: *list /?*

Use the *list volume* option to display information about the disk volumes

To get help on how to load a registry hive into memory from disk, type: *reg load /?*

The following command will load the HKLM registry hive file located in 'D:\Windows\System32\ config\software' into a key file called WindowsSoftware reg load HKLM\WindowsSoftware D:\Windows\System32\config\software

Unload the HKLM\WindowsSoftware registry hive. reg unload HKLM\WindowsSoftware

Reg backup and restore

Backup the entire HKLM registry key to a file called HKLM.reg in the C:\Backup directory. reg export HKLM C:\Backup\HKLM.reg

To create a Registry Hive file backup of the HKLM\Software registry keys reg save HKLM\Software C:\Backup\HKLMSoftware.hiv

Display all the currently available registry PSDrives: Get-PSDrive –PSProvider registry

Display the keys and values under the HKCU\Control Panel key Get-ChildItem "HKCU:\Control Panel" -recurse

Display the keys and values under the HKCU\Control Panel key whose name contains the string "Mouse". Get-ChildItem "HKCU:\Control Panel" -recurse | where name –like "*Mouse*"

Display the content of the HKCU\Control Panel\Mouse\DoubleClickSpeed value. Get-ItemProperty "HKCU:\Control Panel\Mouse" -name DoubleClickSpeed

Notice this value is set to 500. Change the value to 700. Set-ItemProperty "HKCU:\Control Panel\Mouse" –name DoubleClickSpeed –value 700

AD Restore

To find the Windows feature name of the Windows Server Backup, type: Get-WindowsFeature "*backup*"

This should return a single feature, the Windows-Server-Backup feature. To install the feature, type: Get-WindowsFeature "-*backup*" | Install-WindowsFeature

To start a System State backup of the Domain controller, type: wbadmin start systemstatebackup -backupTarget:E: -quiet

To start the server in DSRM mode, type the following command: bcdedit /set safeboot dsrepair and then reboot

non authoritative

The following command will list all of the backup file versions available on the local machine. wbadmin get versions -backuptarget:E:

wbadmin start systemstaterecovery -version:<MM/DD/YYYY-HH:MM> -backuptarget:E: -quiet

Start another command prompt and type: ntdsutil

author itative

Set the local NTDS store as the active instance *activate instance NTDS*

This will start the interactive command environment. Type the following command: authoritative restore

Restore Subtree "OU=Customer Support,OU=Hamilton,DC=Acme,DC=Com"

To remove the 'safeboot' boot option and restart the server normally, open a command prompt and type the following commands: bcdedit /deletevalue safeboot shutdown /r /t 0

Remote management

Remote management (cont)

Get-Command | Where {$_.parameters.keys -like "*ComputerName*"}

Get-service –ComputerName Acmeserver

Get-WmiObject Win32_ComputerSystem –Computername Acmeserver, WINDOW-SCORESERVER

netsh advfirewall firewall set rule group="-Windows Management Instrumentation (WMI)" new enable=yes

Enable-PSRemoting

From the Acmeserver virtual machine, start an Interactive PowerShell session on the Windows81-PC Enter-PSSession Windows81-pc

Install the Web Access gateway role. Install-WindowsFeature –Name WindowsPowerShellWebAccess

To configure the Windows PowerShell Web Access gateway with the default settings using a self-signed certificate, type the following: Install-PswaWebApplication -UseTestCertificate

To see a list of all PSWA cmdlets, type: Get-Command *PSWA* -CommandType cmdlet

The following command will create an authorization rule that will allow the members of the domain admins group access to all of the Domain Controllers in the domain using the default Microsoft.Powershell configuration: Add-PswaAuthorizationRule –userGroupName "acme\domain admins" -ComputerGroupName "acme\Domain Controllers" –ConfigurationName Microsoft.Powershell

New-NetIPAddress –interfaceAlias “Ethernet” –IPAddress 192.168.100.13 –PrefixLength 24
Set-DNSClientServerAddress –InterfaceAlias “Ethernet” –ServerAddresses 192.168.100.10
Add-Computer –DomainName acme –Credential acme\administrator –restart
Type the following commands to enable remote event log management firewall rules: netsh advfirewall firewall set rule group=”Remote Event Log Management” new enable=Yes

By **saadzaf**
cheatography.com/saadzaf/

Published 9th November, 2015.
Last updated 13th May, 2016.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com