

WINDOWS POWERSHELL

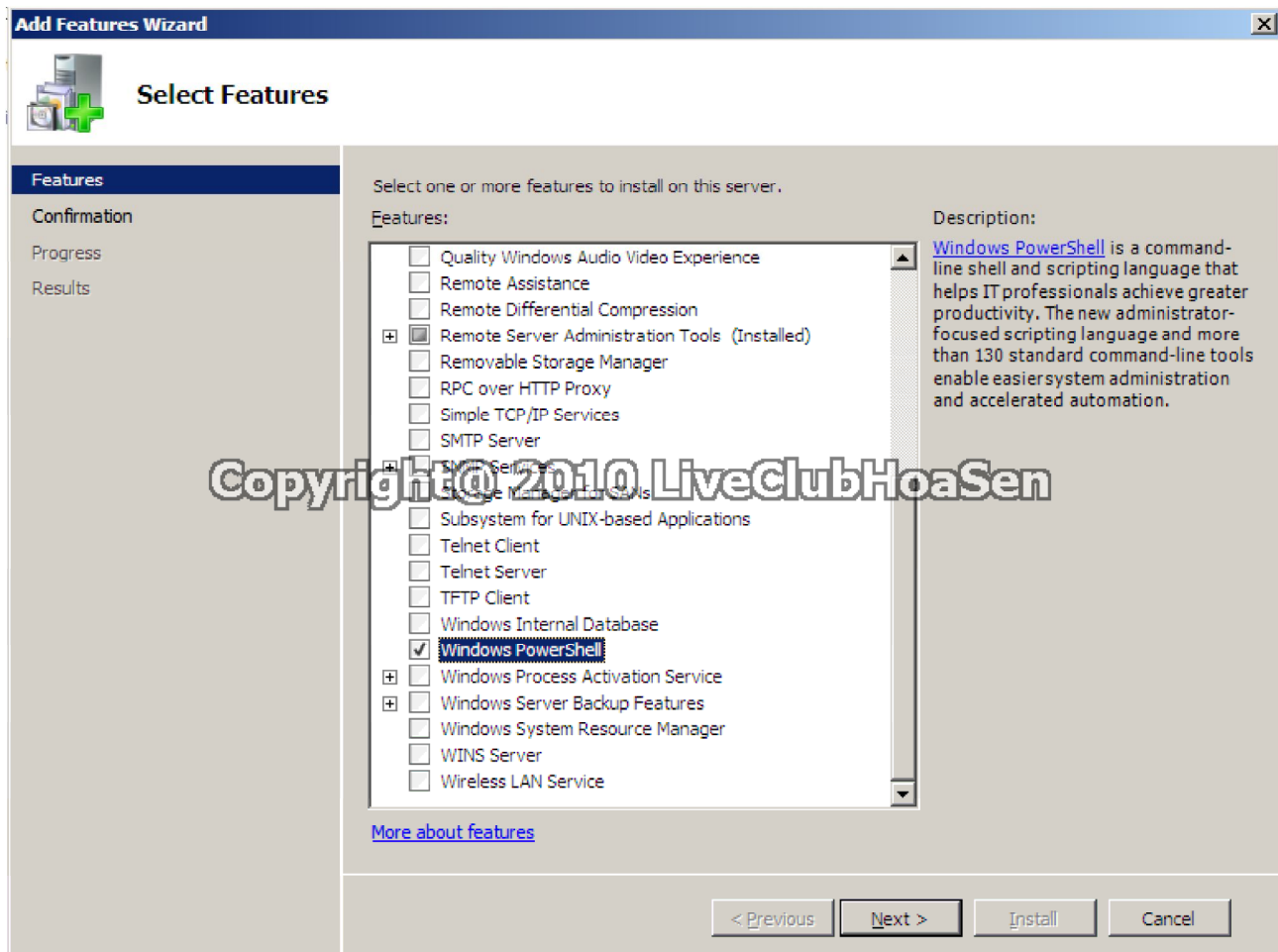
I. Giới thiệu Windows PowerShell

- Windows PowerShell là một môi trường tương tác mới của hệ điều hành Windows, đặc biệt thích hợp với nhiệm vụ quản trị hệ thống. PowerShell này gồm có một công cụ tương tác trên dòng lệnh và một môi trường để thực thi script.
- PowerShell đòi hỏi NET Framework 2.0, phiên bản hiện tại là PowerShell 2.0 được tích hợp sẵn trong phiên bản Windows Server 2008 R2.
- Windows PowerShell bao gồm một khái niệm mới là cmdlet, là một tập hợp các công cụ đơn giản và hữu hiệu được tích hợp trên PowerShell. PowerShell bao gồm hơn 100 cmdlet cơ bản.
- PowerShell còn có khả năng truy cập các file system, registry và các kho lưu trữ khác trên hệ thống.

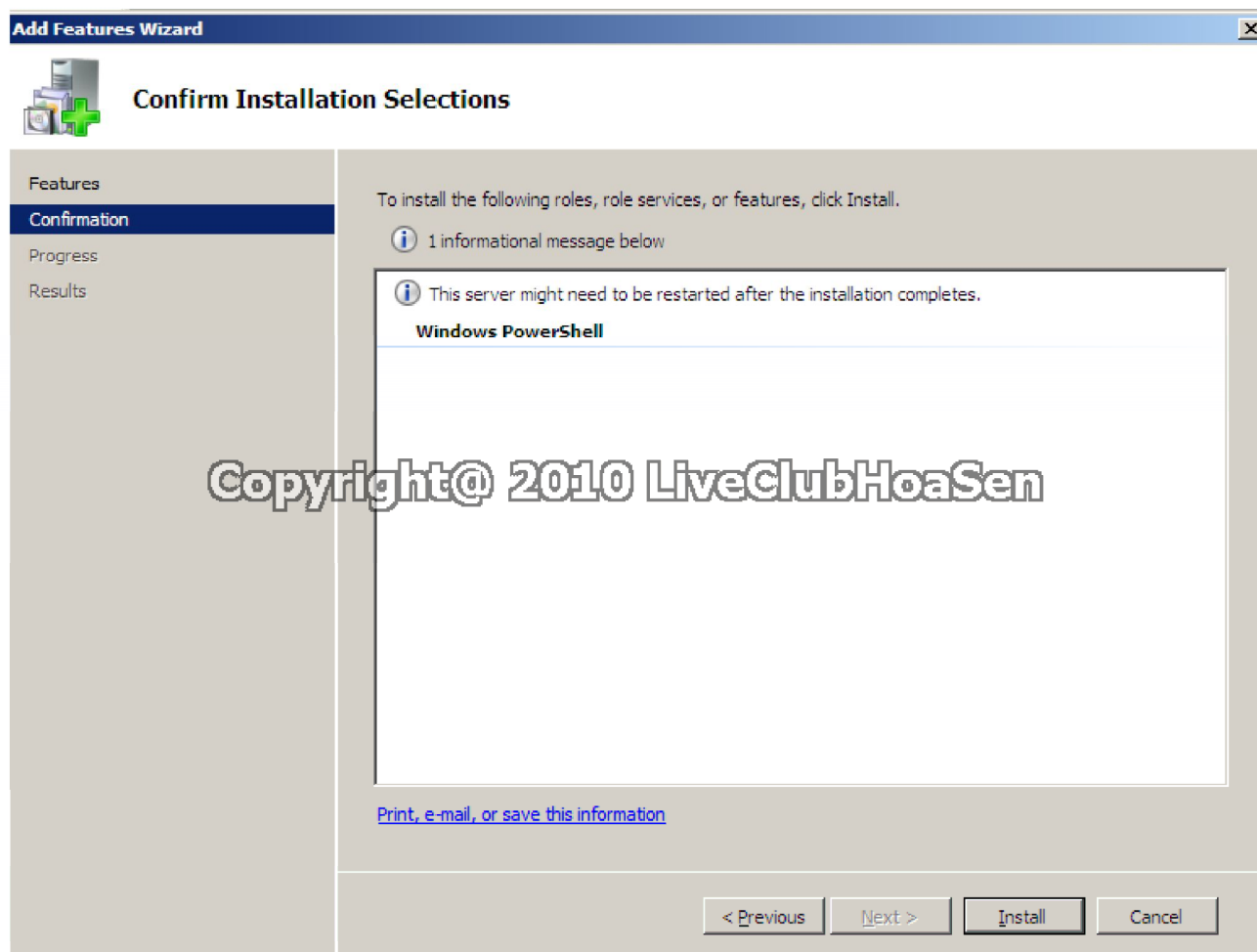
II. Cài đặt Windows PowerShell

Mở cửa sổ **Server Manager**. Trong khung **Features Summary** bên phải chọn **Add Features**.

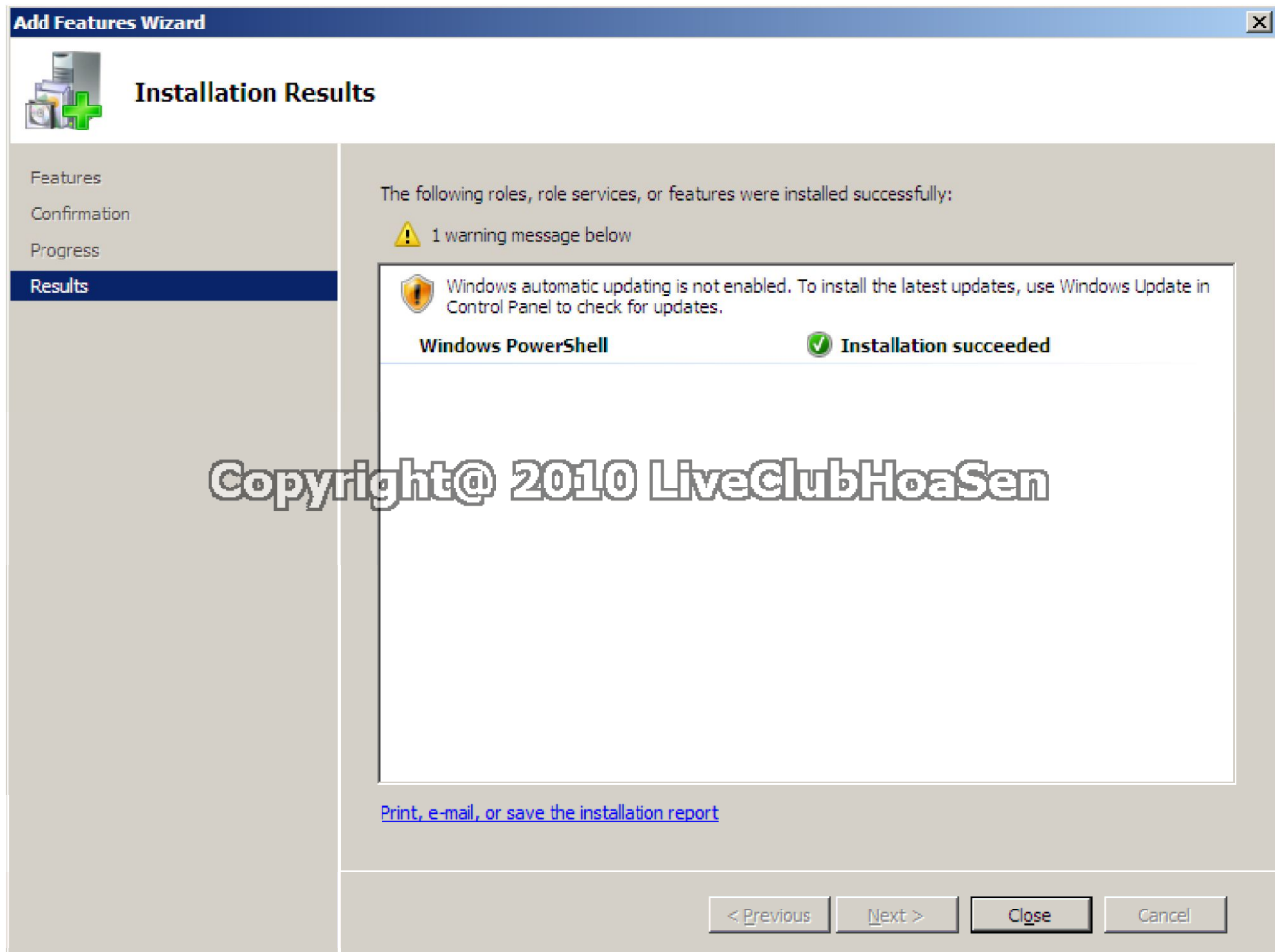
Tiếp đến màn hình **Select Features** -> **Windows PowerShell** -> **Next**



Màn hình **Confirm Installation Selections** -> **Install**

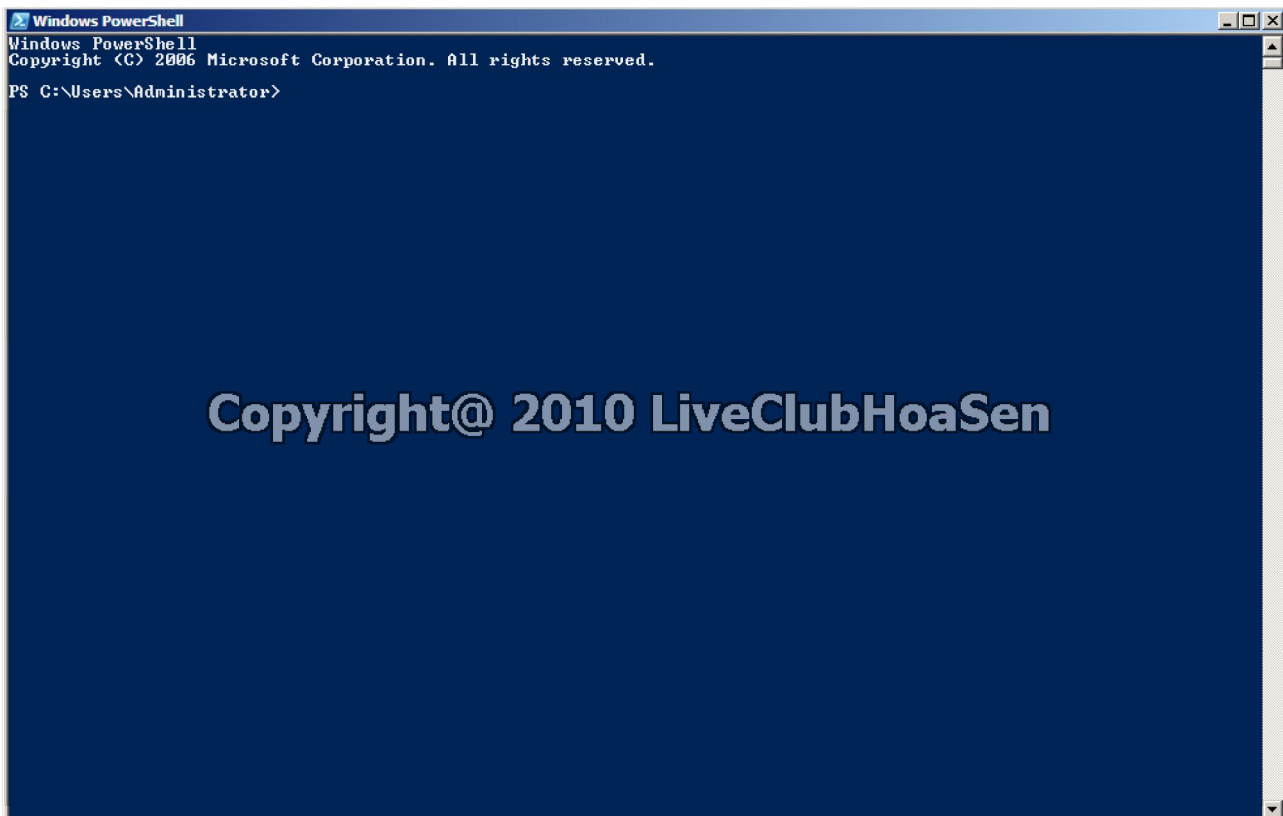


Sau khi tiến trình cài đặt kết thúc, màn hình **Installation Results**, chọn **Close** để hoàn thành quá trình cài đặt.

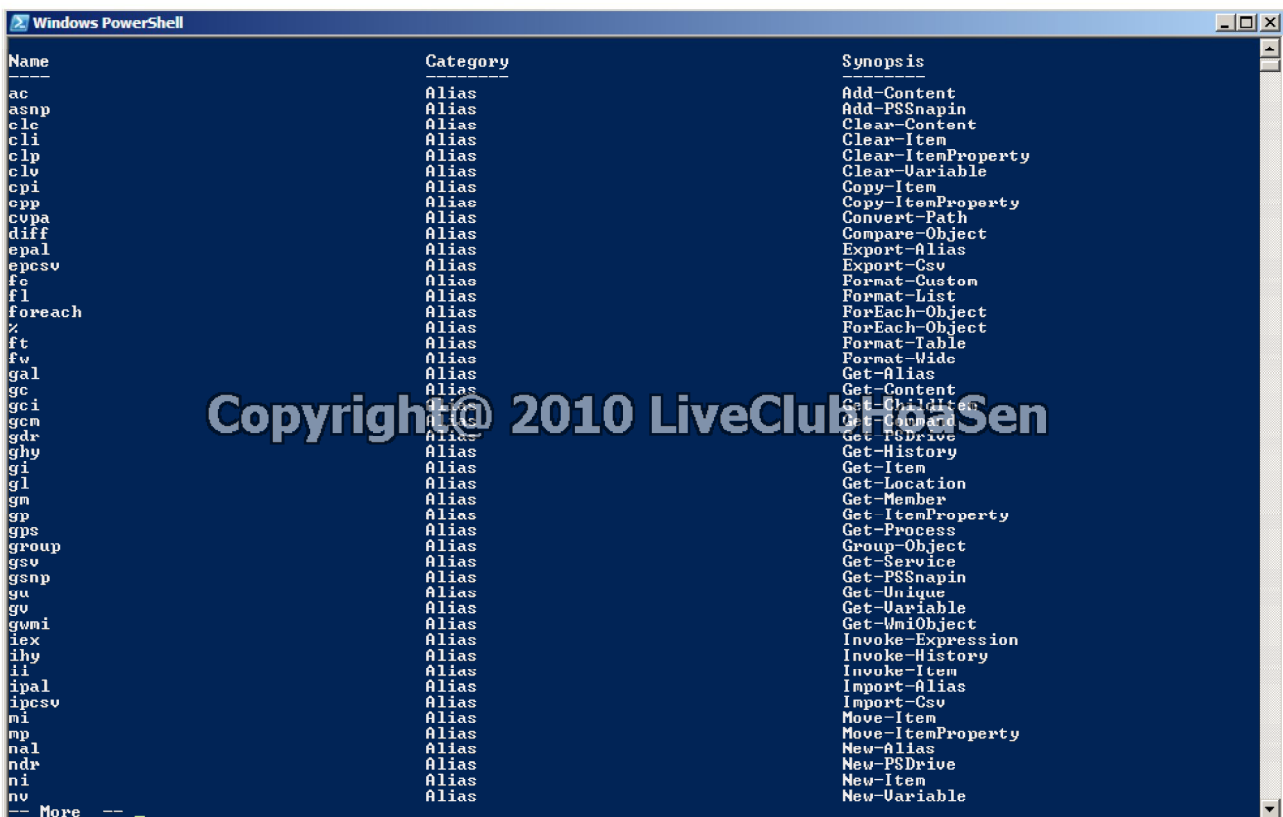


III. Tập lệnh cơ bản trong Windows PowerShell

Đề vào màn hình làm việc Windows PowerShell vào **Start->Programs -> Windows PowerShell 1.0 -> Windows PowerShell**



Để liệt kê danh sách đầy đủ các lệnh hỗ trợ, bạn gõ lệnh **help** -> **Enter**



Tương ứng với mỗi lệnh sẽ có một cmdlet. Ví dụ lệnh **dir** là alias của cmd **Get-ChildItem**

Để lấy thông tin hướng dẫn chi tiết mỗi lệnh, bạn sử dụng cmdlet **Get-Help**

```

Windows PowerShell
PS C:\Users\Administrator> Get-Help Get-ChildItem

NAME
    Get-ChildItem

SYNOPSIS
    Gets the items and child items in one or more specified locations.

SYNTAX
    Get-ChildItem [[-path] <string[]>] [[-filter] <string>] [-include <string[]>] [-exclude <string[]>] [-name] [-recurse] [-force] [<CommonParameters>]

    Get-ChildItem [-literalPath <string[]>] [[-filter] <string>] [-include <string[]>] [-exclude <string[]>] [-name] [-recurse] [-force] [<CommonParameters>]

DETAILED DESCRIPTION
    The Get-ChildItem cmdlet gets the items in one or more specified locations. If the item is a container, it gets the items inside the container, known as child items. You can use the -recurse parameter to get items in all child containers. A location can be a file system location, such as a directory, or a location exposed by another provider, such as a registry hive or a certificate store.

RELATED LINKS
    Get-Item
    Get-Alias
    Get-Location
    Get-Process
    about_namespace

REMARKS
    For more information, type: "get-help Get-ChildItem -detailed".
    For technical information, type: "get-help Get-ChildItem -full".

PS C:\Users\Administrator> _
  
```

Chạy những chương trình ứng dụng bằng câu lệnh

B1: Xuất kết quả của lệnh ipconfig /all ra tập tin ipconfig.txt
 Bạn gõ lệnh ipconfig /all >ipconfig.txt

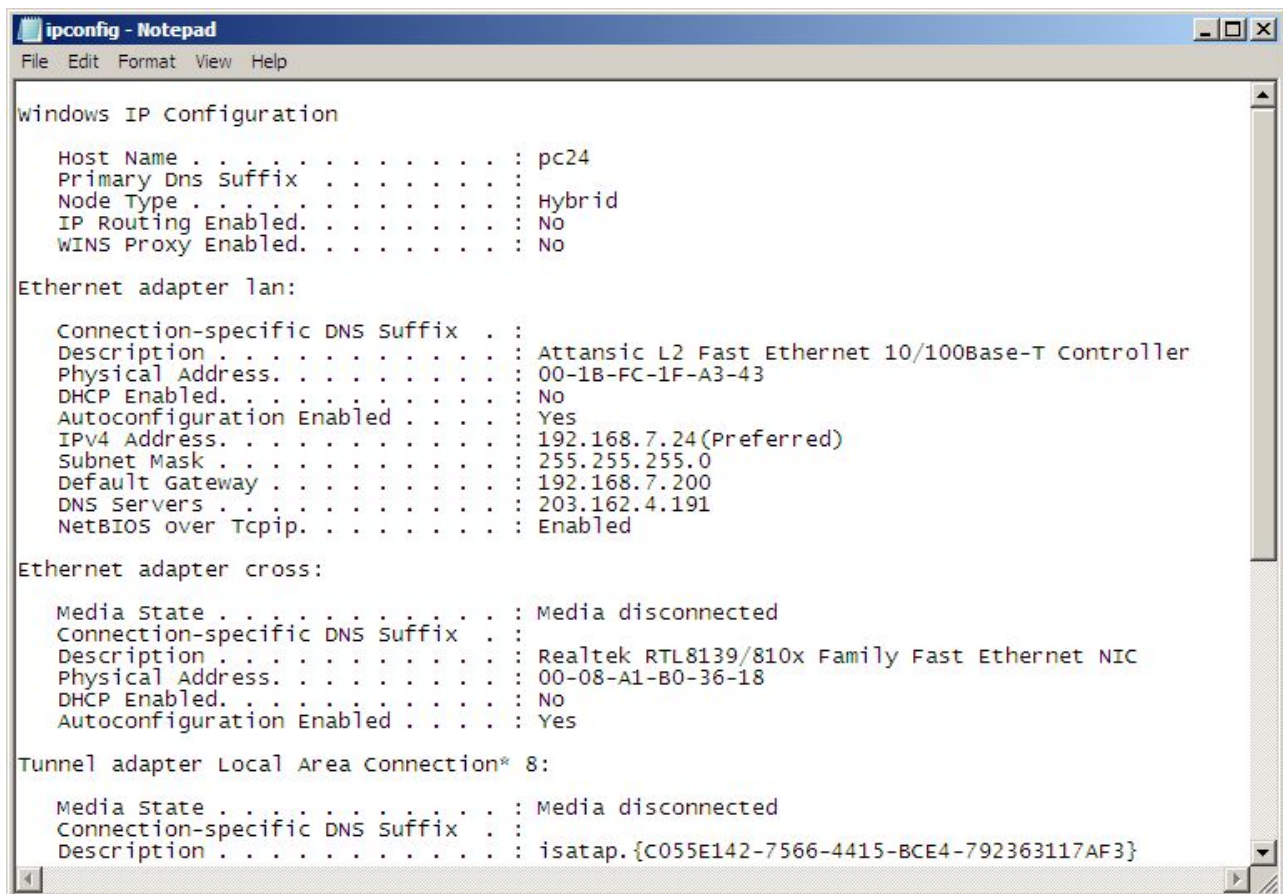
```

Windows PowerShell
PS C:\> ipconfig /all >ipconfig.txt
PS C:\> _
  
```

B2: Chạy file ipconfig.txt bằng notepad
 Bạn gõ lệnh notepad ipconfig.txt

```

Windows PowerShell
PS C:\> notepad ipconfig.txt
PS C:\> _
  
```



```
ipconfig - Notepad
File Edit Format View Help

windows IP Configuration

Host Name . . . . . : pc24
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter lan:

    Connection-specific DNS Suffix . :
    Description . . . . . : Attansic L2 Fast Ethernet 10/100Base-T Controller
    Physical Address. . . . . : 00-1B-FC-1F-A3-43
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.7.24(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.7.200
    DNS Servers . . . . . : 203.162.4.191
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter cross:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
    Physical Address. . . . . : 00-08-A1-B0-36-18
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 8:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : isatap.{C055E142-7566-4415-BCE4-792363117AF3}
```

Tương tự, bạn thử chạy những lệnh khác rồi gán nó vào tập tin để xem thử.

Ngoài các lệnh quen thuộc bạn còn có thể thực hiện các nhiệm vụ quản trị hệ thống thông thường một cách dễ dàng và nhanh chóng bằng những cmdlet. Ví dụ để khắc phục một sự cố trên máy chủ, bạn thường mở cửa sổ Task Manager để xem tiến trình nào đang chạy, ai sử dụng chúng, mỗi tiến trình bao nhiêu RAM và những thông tin liên quan khác. Với PowerShell, bạn chỉ cần sử dụng cmdlet **Get-Process**.

```

Windows PowerShell
PS C:\Users\Administrator> Get-Process

Handles      NPM(K)      PM(K)      WS(K)      UM(M)      CPU(s)      Id ProcessName
-----
452           5        1584        4928        98         1.23       436 csrss
160           6        2472        6924        99         2.67       476 csrss
306          14       16060       14804       71         1.78     1688 dfsrs
151           7        2284        5836        45         0.13       288 dfssvc
237           7        5728       11984        58         1.09     1416 dllhost
217          12       6384       7272         59         0.39     1704 dns
76           3        1272       3932         40         0.73     3144 dwm
433          12       17140      20244       129         5.08     3184 explorer
101           4        9176      12608        42         0.34     2640 iashost
0            0         0         24         0          0         0 Idle
119           6        2620       4556        33         0.09     1724 ismserv
1078         52       21444      24196        81         4.06       572 lsass
160           3        1528       3700        23         0.03       580 lsm
93           3        1972       5648        31         0.22     1072 mscorsvw
173           8        3012       7304        58         0.44       276 msdtc
542          12       50372      50552       178         4.13       564 powershell
273           7        5036       6240        33        16.06       560 services
90           3        5116       9904        28        11.95     1016 SLsvc
28           1         256        684         4         0.48       372 smss
294           2       6332      2564        78         0.44     1632 spoolsv
42           1         340       1084        15         0.02     800 svchost
293           4        4928       5520        31         0.83     800 svchost
275           9        2724       6096        29         0.20     868 svchost
289          10       5412       8020        37         1.58     960 svchost
206           6        3508       7276        34         0.88     984 svchost
909          28       20172      25844       103         3.45    1000 svchost
529           9        5428       8940        51         0.83    1060 svchost
231           8        7020       8116        59         0.16    1128 svchost
425          13       13476      14984        73         0.98    1152 svchost
278          24        7052      10420        45         0.77    1328 svchost
126           5        2124       5276        30         0.13    1948 svchost
73           2         828       2852        21         0.03    1964 svchost
508           0         0        1708         4          0         4 System
181           6        2256       6876        47         0.23    1524 taskeng
237           7        2584       7048        60         0.28    3108 taskeng
256           7       21844      26820        83        30.14    3852 TrustedInstaller
219           5        3128       7664        67         1.70    2020 UMwareService
54           3        1184       3932        50         0.13    3352 UMwareTray
136           5       3796      8552         69         2.89    3364 UMwareUser
100           4        1152       3824        35         0.83       484 wininit
114           3        1168       4128        26         0.42       512 winlogon
141           3       2484       4832        52         0.11    3444 wuaucit

PS C:\Users\Administrator>

```

Kill các process của máy tính:
 Bạn gõ lệnh: kill [số id của chương trình mà bạn muốn kill] .
 Ví dụ trong bảng bên dưới, bạn muốn kill chương trình firefox, bạn nhập lệnh kill 736

Windows PowerShell

PS C:\> get-process

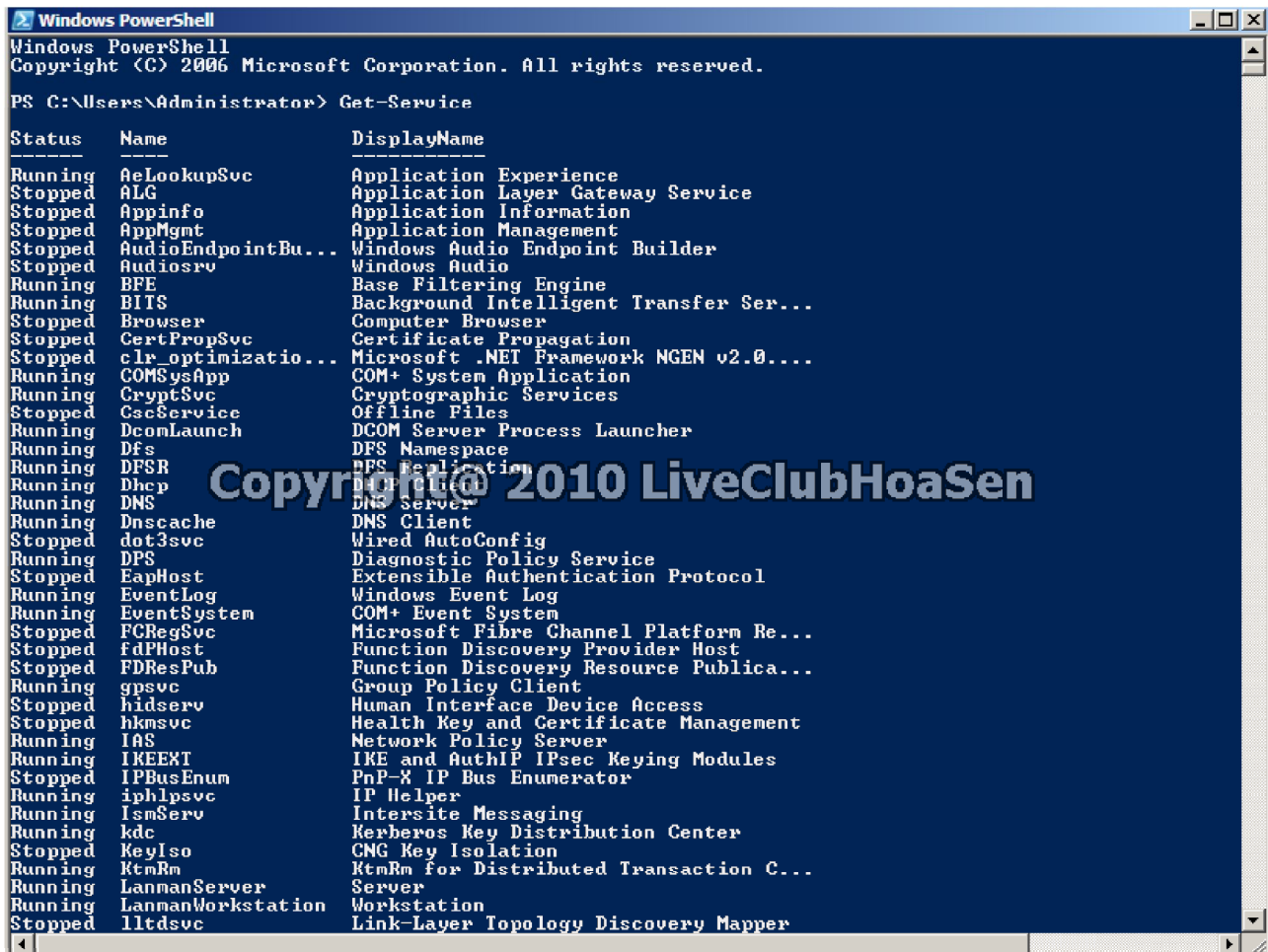
Handles	NPM(K)	PM(K)	WS(K)	UM(M)	CPU(s)	Id	ProcessName
369	5	1696	5124	106	2.22	468	csrss
259	6	2596	9172	109	8.02	512	csrss
80	3	1324	3952	45	0.03	232	dwm
795	17	24836	32188	168	20.42	772	explorer
194	11	26100	36932	117	8.78	736	firefox
58	3	1960	5136	55	2.53	3024	HQScreen
0	0	0	16	0		0	Idle
193	6	6064	9876	74	0.37	2200	IDMan
56	3	2000	4096	60	0.02	2160	issch
570	9	3132	8032	48	2.29	608	lsass
155	3	1504	3668	31	0.00	616	lsn
332	9	6388	9380	90	0.59	2172	MSASCui
170	7	2820	6720	62	0.14	3064	msdtc
688	9	53056	51568	185	3.12	2116	powershell
231	6	2384	6488	43	11.03	596	services
98	3	4980	9380	46	2.34	1016	SLsvc
28	1	288	732	4	0.06	400	smss
283	8	5916	8620	86	0.31	1524	spoolsv
294	5	2120	5380	42	0.81	776	svchost
244	7	2944	5992	39	0.28	836	svchost
336	7	7000	11728	62	2.68	876	svchost
269	9	4996	7452	47	0.37	968	svchost
924	30	17700	21480	106	2.57	992	svchost
271	12	3940	7344	45	0.19	1064	svchost
256	10	7216	8108	70	0.11	1144	svchost
73	2	2016	3388	34	0.02	1164	svchost
395	11	12868	13776	86	0.48	1188	svchost
260	22	4832	8492	49	0.30	1308	svchost
101	4	1536	4220	49	0.02	1384	svchost
122	6	1500	4484	37	0.08	1676	svchost
74	2	820	2840	29	0.00	1688	svchost
47	1	564	2196	15	0.00	1856	svchost
229	7	3256	4860	48	0.03	2712	svchost
532	0	0	2972	5		4	System
134	5	1836	5396	52	0.09	1708	taskeng
247	7	2748	6944	64	0.12	1760	taskeng
104	4	1152	3876	44	0.78	520	wininit
119	3	1240	4152	30	0.56	556	winlogon
52	3	2740	5060	63	0.08	2980	Ymsgr_tray

Windows PowerShell

PS C:\> kill 736

PS C:\>

Để theo dõi, giám sát các services đang chạy trên hệ thống ta có thể sử dụng lệnh **Get-Service**



```

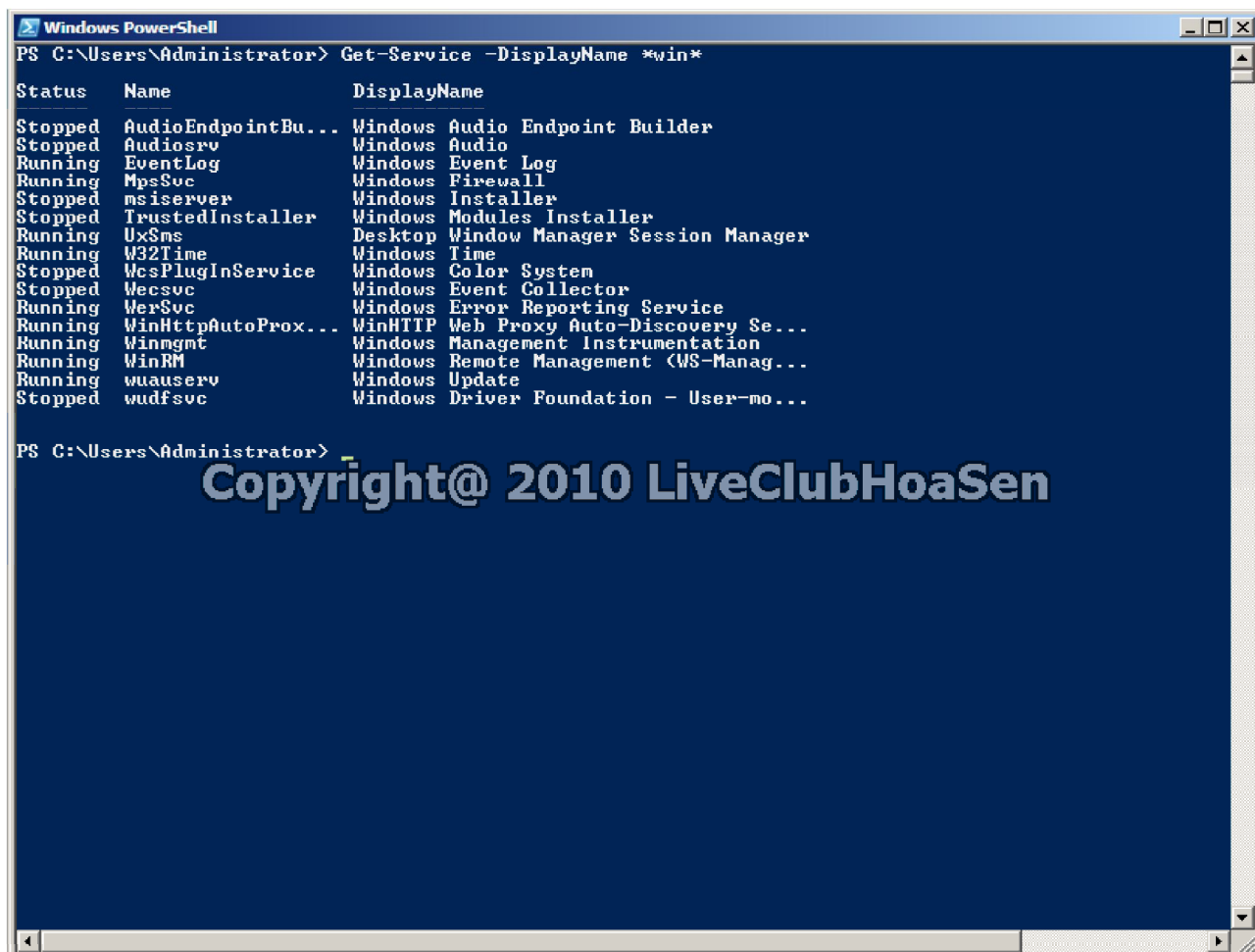
Windows PowerShell
Copyright (C) 2006 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-Service

Status      Name                      DisplayName
-----
Running     AeLookupSvc              Application Experience
Stopped     ALG                      Application Layer Gateway Service
Stopped     Appinfo                  Application Information
Stopped     AppMgmt                  Application Management
Stopped     AudioEndpointBuilder     Windows Audio Endpoint Builder
Stopped     Audiosrv                 Windows Audio
Running     BFE                      Base Filtering Engine
Running     BITS                     Background Intelligent Transfer Ser...
Stopped     Browser                  Computer Browser
Stopped     CertPropSvc              Certificate Propagation
Stopped     clr_optimizatio...       Microsoft .NET Framework NGEN v2.0....
Running     COMSysApp                COM+ System Application
Running     CryptSvc                 Cryptographic Services
Stopped     CscService               Offline Files
Running     DcomLaunch               DCOM Server Process Launcher
Running     Dfs                      DFS Namespace
Running     Dfsr                     DFS Replication
Running     Dhcp                     DHCP Server
Running     DNS                      DNS Server
Running     Dnscache                 DNS Client
Stopped     dot3svc                  Wired AutoConfig
Running     DPS                      Diagnostic Policy Service
Stopped     EapHost                  Extensible Authentication Protocol
Running     EventLog                 Windows Event Log
Running     EventSystem              COM+ Event System
Stopped     FCRegSvc                 Microsoft Fibre Channel Platform Re...
Stopped     fdPHost                  Function Discovery Provider Host
Stopped     FDResPub                 Function Discovery Resource Publica...
Running     gpsvc                    Group Policy Client
Stopped     hidserv                  Human Interface Device Access
Stopped     hkmsvc                   Health Key and Certificate Management
Running     IAS                      Network Policy Server
Running     IKEEXT                   IKE and AuthIP IPsec Keying Modules
Stopped     IPBusEnum                PnP-X IP Bus Enumerator
Running     iphlpsvc                 IP Helper
Running     lsmSvc                   Intersite Messaging
Running     kdc                      Kerberos Key Distribution Center
Stopped     KeyIso                   CNG Key Isolation
Running     KtmRm                    KtmRm for Distributed Transaction C...
Running     LanmanServer              Server
Running     LanmanWorkstation         Workstation
Stopped     lltdsvc                  Link-Layer Topology Discovery Mapper

```

Ngoài ra nếu muốn hiển thị một số dịch vụ cụ thể, bạn có thể sử dụng các ký tự đại diện. Ví dụ để hiển thị các dịch vụ có tên hiển thị chứa chuỗi “win”, ta thực hiện lệnh sau **Get-Service -displayname *win***



```
Windows PowerShell
PS C:\Users\Administrator> Get-Service -DisplayName *win*

Status      Name                DisplayName
-----
Stopped     AudioEndpointBu...  Windows Audio Endpoint Builder
Stopped     Audiosrv            Windows Audio
Running     EventLog            Windows Event Log
Running     MpsSvc              Windows Firewall
Stopped     msiserver            Windows Installer
Stopped     TrustedInstaller    Windows Modules Installer
Running     UxSms               Desktop Window Manager Session Manager
Running     W32Time             Windows Time
Stopped     WcsPlugInService    Windows Color System
Stopped     Wecsvc              Windows Event Collector
Running     Wersvc              Windows Error Reporting Service
Running     WinHttpAutoProx...  WinHTTP Web Proxy Auto-Discovery Se...
Running     Winmgmt              Windows Management Instrumentation
Running     WinRM               Windows Remote Management (WS-Manag...
Running     wuauserv             Windows Update
Stopped     wudfsvc              Windows Driver Foundation - User-mo...
```

* Xem thông tin về CPU

Bạn gõ lệnh: `get-wmiobject -class win32_processor`

```
Windows PowerShell
PS C:\> get-wmiobject -class win32_processor

GENUS           : 2
CLASS           : Win32_Processor
SUPERCLASS      : CIM_Processor
DYNASTY         : CIM_ManagedSystemElement
RELPATH         : Win32_Processor.DeviceID="CPU0"
PROPERTY_COUNT  : 48
DERIVATION      : <CIM_Processor, CIM_LogicalDevice, CIM_LogicalElement, CIM_ManagedSystemElement>
SERVER         : PC24
NAMESPACE      : root\cimv2
PATH           : \\PC24\root\cimv2:Win32_Processor.DeviceID="CPU0"
AddressWidth    : 32
Architecture    : 9
Availability    : 3
Caption        : x64 Family 6 Model 15 Stepping 2
ConfigManagerErrorCode : 
ConfigManagerUserConfig : 
CpuStatus       : 1
CreationClassName : Win32_Processor
CurrentClockSpeed : 1200
CurrentVoltage  : 14
DataWidth      : 64
Description     : x64 Family 6 Model 15 Stepping 2
DeviceID        : CPU0
ErrorCleared    : 
ErrorDescription : 
ExtClock       : 200
Family         : 178
InstallDate    : 
L2CacheSize    : 1024
L2CacheSpeed   : 
L3CacheSize    : 0
L3CacheSpeed   : 0
LastErrorCode   : 
Level          : 6
LoadPercentage  : 0
Manufacturer    : GenuineIntel
MaxClockSpeed   : 1600
Name           : Genuine Intel(R) CPU           2140  @ 1.60GHz
NumberOfCores   : 2
NumberOfLogicalProcessors : 2
OtherFamilyDescription : 
PNPDeviceID     : 
PowerManagementCapabilities : 
PowerManagementSupported : False
ProcessorId     : BFEBFBFF000006F2
ProcessorType   : 3
Revision       : 3842
```

Xem thông tin về hệ điều hành

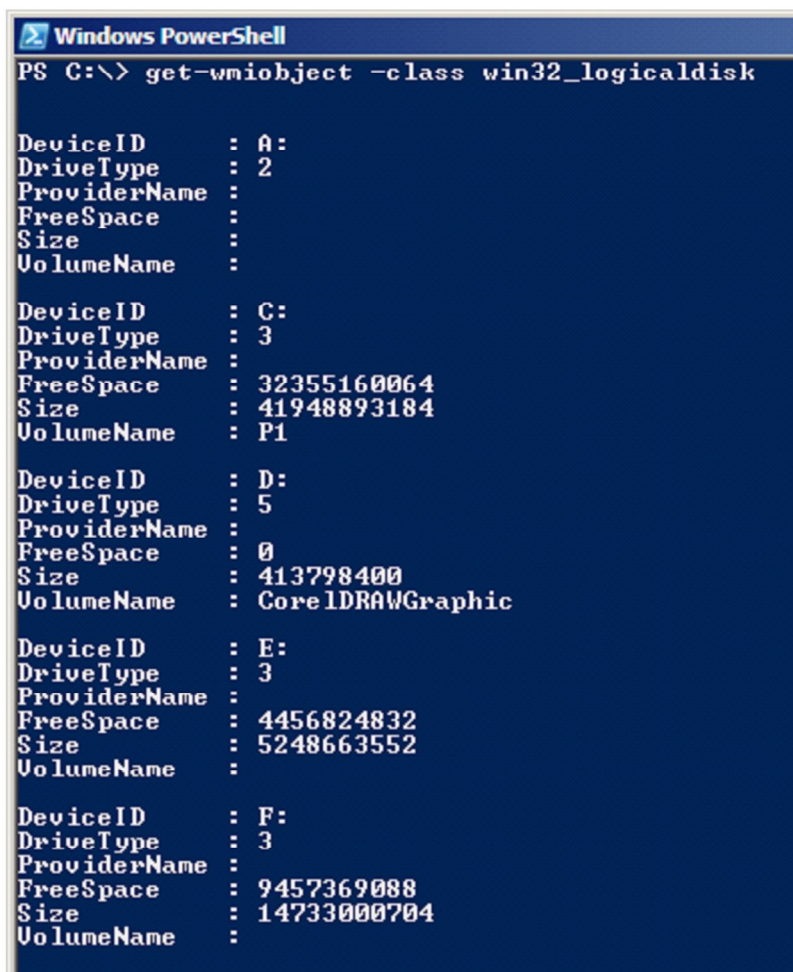
Bạn gõ lệnh: `get-wmiobject -class win32_operatingsystem`

```
Windows PowerShell
PS C:\> get-wmiobject -class win32_operatingsystem

SystemDirectory : C:\Windows\system32
Organization    : 
BuildNumber     : 6001
RegisteredUser  : Windows User
SerialNumber    : 78440-047-2885973-70154
Version        : 6.0.6001
```

Xem thông tin về ổ đĩa :

Bạn gõ lệnh: `get-wmiobject -class win32_logicaldisk`



```
Windows PowerShell
PS C:\> get-wmiobject -class win32_logicaldisk

DeviceID      : A:
DriveType     : 2
ProviderName  :
FreeSpace     :
Size         :
VolumeName    :

DeviceID      : C:
DriveType     : 3
ProviderName  :
FreeSpace     : 32355160064
Size         : 41948893184
VolumeName    : P1

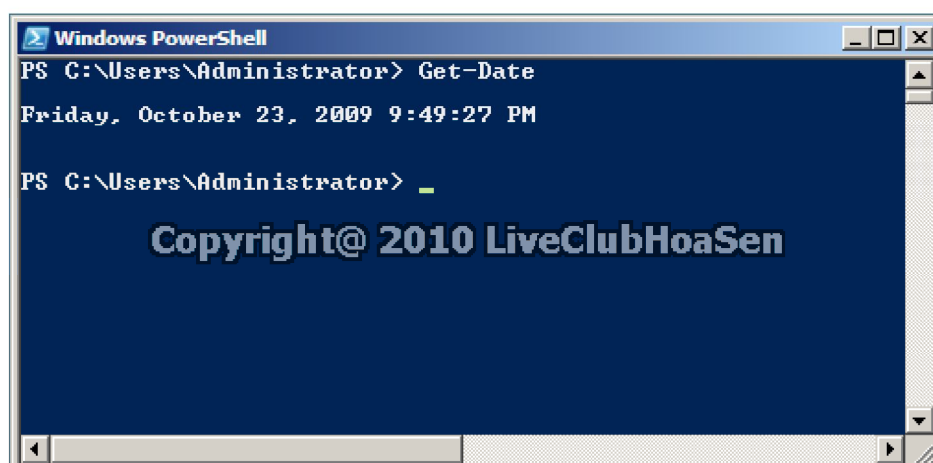
DeviceID      : D:
DriveType     : 5
ProviderName  :
FreeSpace     : 0
Size         : 413798400
VolumeName    : CoreIDRAWGraphic

DeviceID      : E:
DriveType     : 3
ProviderName  :
FreeSpace     : 4456824832
Size         : 5248663552
VolumeName    :

DeviceID      : F:
DriveType     : 3
ProviderName  :
FreeSpace     : 9457369088
Size         : 14733000704
VolumeName    :
```

Cmdlet được gọi theo dạng verb-noun, sẽ cho biết rằng lệnh đó làm gì và với đối tượng nào.

Ví dụ cmdlet **Get-Date** sẽ hiện thị thông tin ngày giờ hệ thống, **Set-Date** sẽ thiết lập ngày giờ hệ thống

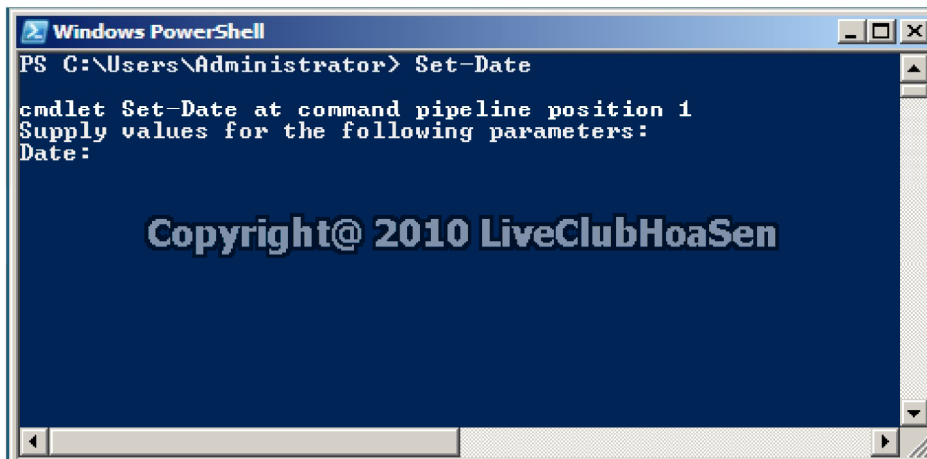


```
Windows PowerShell
PS C:\Users\Administrator> Get-Date

Friday, October 23, 2009 9:49:27 PM

PS C:\Users\Administrator> _

Copyright@ 2010 LiveClubHoaSen
```



Bên cạnh đó, Windows PowerShell cũng tách biệt giữa dữ liệu và cách hiển thị dữ liệu đó, được định dạng cho dễ đọc.

IV. Windows PowerShell Script

Bạn có thể sử dụng PowerShell để xây dựng các script, nó cung cấp cho bạn một ngôn ngữ script với các phép lặp và các phép toán logic hoàn hảo. Cú pháp của script tương tự các ngôn ngữ lập trình .NET như C#

Hướng dẫn xây dựng 1 script căn bản

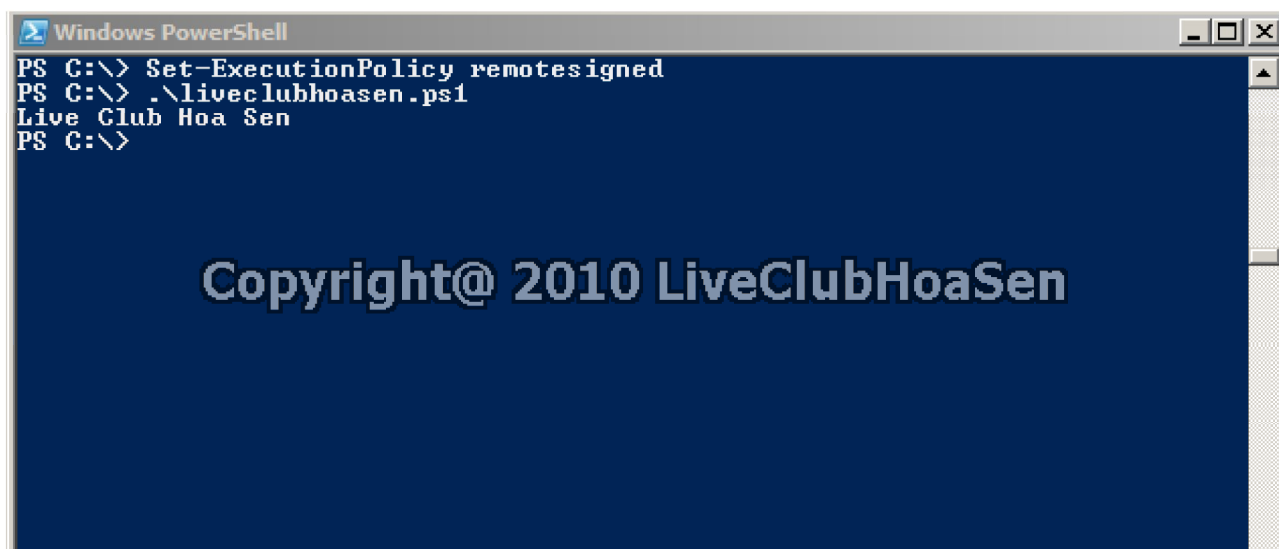
1. Mở Notepad và soạn đoạn mã sau:

```
$a = "LiveClub Hoa Sen"
```

```
Write-host $a
```

2. Lưu file C:\liveclubhoasen.ps1
3. Thay đổi chính sách thực thi sang RemoteSigned để các script nội bộ có thể thực thi Set-ExecutionPolicy RemoteSigned
4. Tại cửa sổ Windows PowerShell, nhập C:\liveclubhoasen.ps1

Nếu dòng "LiveClub Hoa Sen" hiển thị, bạn đã hoàn thành việc xây dựng script.



The screenshot shows a Windows PowerShell window with a dark blue background. The title bar reads "Windows PowerShell". The command history shows the following commands and output:

```
PS C:\> Set-ExecutionPolicy remotesigned
PS C:\> .\liveclubhoasen.ps1
Live Club Hoa Sen
PS C:\>
```

Below the command history, a large, bold, white text message is displayed:

Copyright@ 2010 LiveClubHoaSen