

Presentación de Windows PowerShell

1. Introducción	15
2. ¿ Qué es Windows PowerShell ?	19
3. ¿ Y los scripts, en todo esto ?	20
4. La sintaxis de Windows PowerShell	21
4.1 Encontrar rápidamente un cmdlet	23
4.2 Obtener la documentación de un cmdlet	24
4.3 Actualizar la documentación	26
5. Las distintas versiones de Windows PowerShell	26
5.1 Versión 1.0	26
5.2 Versión 2.0	27
5.3 Versión 3.0	28
5.4 Versión 4.0	29
5.5 Versión 5.0 y 5.1	30
5.6 Evolución continua de Windows PowerShell	32
6. Conocer la versión de PowerShell instalada	33

Las unidades de Windows PowerShell

1. Las unidades de Windows PowerShell y la navegación	37
1.1 ¿ Qué es una unidad Windows PowerShell ?	37
1.2 Conocer las unidades de Windows PowerShell accesibles	38
2. El sistema de archivos	41
2.1 Cmdlets dedicados a la navegación	41
2.1.1 Get-Location	42
2.1.2 Set-Location	42
2.1.3 Get-ChildItem	42
2.2 Cmdlets dedicados a la manipulación	45
2.2.1 Get-Item	45
2.2.2 Get-Content	47
2.2.3 Set-Content	49
2.2.4 New-Item	50
2.2.5 Remove-Item	51
2.2.6 Copy-Item	52
2.2.7 Rename-Item	53
2.2.8 Move-Item	54
2.2.9 Invoke-Item	

	55
3. El registro de Windows (HKCU y HKLM)	56
3.1 Moverse por el registro	57
3.2 Crear una clave del registro	58
3.3 Crear un valor del registro	58
3.4 Recuperar el dato de un valor del registro	60
3.5 Borrar el dato de un valor del registro	61
3.6 Renombrar un valor del registro	62
3.7 Mover un valor del registro	62
3.8 Copiar un valor del registro	63
3.9 Eliminar un valor del registro	64
3.10 Eliminar una clave del registro	64
4. Los certificados	65
4.1 Gestionar los certificados con Windows PowerShell	66
4.2 Crear certificados autofirmados	70
4.2.1 Crear un nuevo certificado	71
4.2.2 Clonar un certificado	71
4.3 Exportar certificados	72
4.4 Importar certificados	75
5. Web Services-Management	

	76
6. Internet Information Services (IIS)	78
6.1 Interactuar con los pools de aplicaciones	81
6.2 Los sitios web	83
6.3 Copia de seguridad y restauración	87
6.3.1 Copia de seguridad de la configuración de IIS	87
6.3.2 Copia de seguridad de los datos de los sitios web	88
Sistema y características	
1. Introducción	89
2. Las características de Windows	89
2.1 Activar una característica	93
2.2 Desactivar una característica	94
3. Las aplicaciones de Windows Store	95
3.1 Instalar una app	98
3.2 Eliminar una app	98
4. Los procesos	100
4.1 Obtener la lista de procesos	101

4.2 Detener un proceso	106
4.3 Arrancar un proceso	108
4.4 Arrancar una app	109
5. Los servicios	110
5.1 Manipulaciones básicas	111
5.1.1 Obtener información acerca de los servicios	111
5.1.2 Arrancar un servicio	114
5.1.3 Reiniciar un servicio	115
5.1.4 Detener un servicio	115
5.2 Operaciones avanzadas	117
5.2.1 Crear un nuevo servicio	117
5.2.2 Modificar un servicio existente	119
5.2.3 Eliminar un servicio	119
6. El equipo y el sistema operativo	120
6.1 Renombrar el equipo	120
6.2 Reiniciar el equipo	123
6.3 Detener el equipo	126
6.4 Unirse a un dominio	127
6.5 Sacar del dominio	130
6.6 Cambiar de dominio o de grupo de trabajo	

1.8 Eliminar del registro una tarea planificada	161
	162
2. Los registros de eventos	163
2.1 Obtener información acerca de los eventos	166
2.2 Administrar los registros de eventos	173
2.3 Borrar el contenido de un registro de eventos	175
2.4 Escribir un evento en un registro de eventos	177
3. Los parámetros regionales y de idioma	179
3.1 Obtener los parámetros regionales	182
3.2 Obtener el idioma de la interfaz gráfica	183
3.3 Modificar los parámetros regionales	184
3.4 Idioma	187
3.4.1 Obtener las preferencias de idioma	187
3.4.2 Modificar las preferencias de idioma	188
3.4.3 Instanciar un nuevo idioma	192
3.5 Ubicación	193
3.5.1 Obtener la ubicación	193
3.5.2 Configurar la ubicación	193
4. Compresión de archivos	196

4.1 Compresión	197
4.2 Descompresión	200

Seguridad y protección

1. La seguridad y el Firewall de Windows	201
1.1 Activar el Firewall de Windows	203
1.2 Desactivar el Firewall de Windows	206
1.3 Crear una nueva regla de seguridad	206
1.4 Administrar los logs	210
1.5 Cambiar de perfil de red	212
1.5.1 Obtener la lista de conexiones activas y el tipo de perfil asociado	215
1.5.2 Cambiar el tipo de perfil de la conexión activa	216
2. Windows Defender	217
2.1 Recuperar la información de Windows Defender	219
2.2 Actualizar las definiciones del antimalware y del antivirus	223
2.3 Administrar los análisis de Windows Defender	224
2.4 Administrar las amenazas detectadas	227
2.4.1 Recuperar los eventos ligados a la detección de amenazas	227
2.4.2 Recuperar el histórico de amenazas detectadas	229
2.5 Limpiar o eliminar las amenazas detectadas	

2.6 Consultar el catálogo de amenazas	230
2.7 Administrar los parámetros y las preferencias	231
2.7.1 Obtener la configuración y los parámetros	232
2.7.2 Modificar la configuración y los parámetros	233
2.7.3 Agregar y eliminar exclusiones	234
3. Administrar usuarios y grupos locales	241
3.1 Usuarios	243
3.1.1 Obtener la lista de cuentas de usuario	244
3.1.2 Crear una cuenta de usuario local	245
3.1.3 Modificar una cuenta de usuario local	246
3.1.4 Renombrar una cuenta de usuario local	248
3.1.5 Activar una cuenta de usuario local	249
3.1.6 Desactivar una cuenta de usuario local	250
3.1.7 Eliminar una cuenta de usuario local	251
3.2 Grupos	251
3.2.1 Obtener la lista de grupos locales	252
3.2.2 Crear un grupo local	253
3.2.3 Modificar las propiedades de un grupo local	254
3.2.4 Renombrar un grupo local	256
3.2.5 Eliminar un grupo local	257

3.3 Administrar los miembros de los grupos locales	258
3.3.1 Agregar miembros en un grupo local	258
3.3.2 Obtener los miembros presentes en un grupo local	259
3.3.3 Eliminar miembros de un grupo local	260
4. Compartición de carpetas	261
4.1 Crear un recurso compartido de red	262
4.2 Recuperar información de los recursos compartidos de red	264
4.3 Modificar un recurso compartido de red existente	267
4.4 Eliminar un recurso compartido de red	269
4.5 Administrar los permisos del recurso compartido SMB	270
4.5.1 Recuperar los permisos del recurso compartido	271
4.5.2 Agregar o revocar permisos de acceso al recurso compartido	271
4.5.3 Bloquear o desbloquear permisos de acceso al recurso compartido	272
	276
Buscar y recopilar información	
1. Introducción	279
2. Buscar archivos	280
2.1 Buscar archivos en función de sus propiedades	280

2.2 Utilizar el resultado de la búsqueda	282
2.3 Buscar en el contenido de los archivos	283
3. Comparar objetos	284
3.1 Comparar dos archivos de texto	285
3.2 Comparar dos archivos de datos	286
4. Recuperar la información general del equipo	290
5. Las variables de entorno	298
6. Obtener información gracias a las clases WMI	301
6.1 El cmdlet Get-WmiObject	302
6.2 Explotar algunas clases WMI	303
6.2.1 Información vinculada a la BIOS	304
6.2.2 Información vinculada al equipo que trabaja con Windows	306
6.2.3 Información vinculada al equipo (producto)	307
6.2.4 Información vinculada al procesador (CPU)	308
6.2.5 Información vinculada a los discos	309
6.2.6 Información vinculada a los servicios	311
6.2.7 Información vinculada a las carpetas compartidas	312
6.2.8 Información vinculada a los comandos de arranque	314
6.2.9 Información vinculada al sistema operativo	314

6.2.10 Información vinculada a la unidad de CD/DVD	315
6.2.11 Información vinculada a la placa base	317
6.2.12 Información vinculada a la batería	318
6.2.13 Información vinculada a la tarjeta de red	319
6.2.14 Información vinculada a la memoria	320
6.2.15 Información vinculada a las aplicaciones	321
7. Actualizaciones	322
7.1 Mostrar las actualizaciones instaladas	323
7.2 Interactuar con las actualizaciones con wusa.exe	327
7.2.1 Instalar una actualización	328
7.2.2 Desinstalar una actualización	328
Administrar el hardware y los dispositivos	
1. Introducción	329
2. Las tarjetas de red	329
2.1 Realizar un ping	331
2.2 Modificar los parámetros de la tarjeta de red	333
2.2.1 Parametrizar la configuración IP	333

2.2.2 Parametrizar la configuración DNS	346
2.3 Resolución de nombres DNS	350
2.4 Consultar la caché DNS	353
2.5 Renovar la inscripción del cliente DNS	357
2.6 Las conexiones VPN	357
2.6.1 Crear una conexión VPN	357
2.6.2 Modificar una conexión VPN	363
2.6.3 Eliminar una conexión VPN	366
3. La gestión de discos	366
3.1 Los discos duros	368
3.1.1 Redimensionar una partición	369
3.1.2 Crear una nueva partición	371
3.1.3 Formatear una partición	372
3.1.4 Asignar una letra de unidad a una partición	374
3.1.5 Eliminar la letra de unidad de una partición	375
3.1.6 Inicializar un disco	376
3.1.7 Modificar las propiedades de un disco	378
3.1.8 Limpiar un disco	379
3.1.9 Optimizar una partición	380
3.1.10 Corregir los errores de una partición	382

3.1.11 Eliminar una partición	383
3.2 Los discos duros virtuales	384
3.2.1 Crear un disco duro virtual	386
3.2.2 Montar un disco duro virtual	389
3.2.3 Compactar un disco duro virtual de tipo extensión dinámica	390
3.2.4 Convertir un disco duro virtual	391
3.2.5 Redimensionar un disco duro virtual	393
4. La gestión de la energía	394
4.1 Mostrar los planes de energía	394
4.2 Escoger un plan de energía	396
5. La gestión de las impresoras	397
5.1 Los controladores de impresión	398
5.1.1 Conocer los controladores de impresión instalados	398
5.1.2 Agregar un controlador de impresión	399
5.1.3 Eliminar un controlador de impresión	402
5.2 Los puertos de impresión	403
5.2.1 Obtener la lista de puertos	403
5.2.2 Crear un nuevo puerto	404
5.2.3 Eliminar un puerto	405
5.3 Las impresoras	

5.3.1 Agregar una impresora	406
5.3.2 Modificar los parámetros de una impresora	406
5.3.3 Renombrar una impresora	409
5.3.4 Eliminar una impresora	410
5.3.5 Definir una impresora predeterminada	411

Administrar aplicaciones

1. Administrar las aplicaciones instaladas	415
1.1 Enumerar las aplicaciones instaladas	417
1.2 Filtrar las consultas	419
1.2.1 Filtrar por nombre	419
1.2.2 Filtrar por fabricante	420
1.3 Desinstalar una aplicación	421
2. Lanzar un ejecutable	422
3. Windows Installer (MSI)	423
3.1 ¿ Qué es Windows Installer ?	424
3.2 Instalar un paquete MSI	425
3.3 Aplicar una actualización (.msp)	427

3.4 Desinstalar una aplicación con un paquete MSI	427
---	-----

Administrador de paquetes

1. Presentación	429
1.1 Arquitectura	430
1.2 El módulo Package Management	430
1.2.1 Encontrar un paquete	430
1.2.2 Instalar paquetes	431
1.2.3 Herramienta de inventario	432
2. Requisitos previos y funcionamiento	433
3. Descripción de los cmdlets y demostración	434
3.1 Agregar un proveedor de paquetes	435
3.2 Buscar un paquete	436
3.3 Instalar un paquete	440
3.4 Actualizar un paquete	443
3.5 Desinstalar un paquete	443
3.6 Mostrar el conjunto de programas instalados (auditoría)	445
4. Escenarios de uso	447

Administración remota de puestos de trabajo

1. Introducción	449
2. La comunicación remota del Framework .NET	449
2.1 Los cmdlets de comunicación remota del Framework .NET	450
2.2 Algunos ejemplos de envío remoto de comandos	453
3. Administración remota con Windows PowerShell	456
3.1 ¿ Qué es PowerShell Remoting ?	457
3.2 Funcionamiento de PowerShell Remoting	458
3.3 Requisitos previos	460
3.4 Activar PowerShell Remoting	461
3.5 Los métodos de autenticación	463
4. Administración remota	465
4.1 Los distintos tipos de sesiones remotas	466
4.2 Las sesiones permanentes	466
4.2.1 Crear una sesión permanente de manera remota	466
4.2.2 Obtener la lista de sesiones permanentes abiertas	468
4.2.3 Eliminar una sesión permanente de manera remota	469

4.3 Abrir una sesión interactiva de PowerShell remota	470
4.4 Ejecución remota de un comando	472
4.5 Ejecutar scripts de manera remota	475

Scripting

1. Seguridad	479
1.1 ¿ Por qué es importante la seguridad ?	479
1.2 ¿ Cuáles son los riesgos ?	480
1.3 Optimizar la seguridad de ejecución de los scripts	480
1.3.1 Los archivos de script Windows PowerShell (.ps1)	481
1.3.2 Las directivas de ejecución	482
1.3.3 Conocer la directiva de ejecución en curso	483
1.3.4 Cambiar de directiva de ejecución	483
1.4 Implementar las directivas de ejecución por GPO	484
2. Windows PowerShell ISE	485
2.1 Las buenas prácticas del scripting	485
2.2 Paso de parámetros	487
2.2.1 Los parámetros de los scripts	487
2.2.2 Los parámetros de las funciones	488
2.3 Depurar	

	488
3. Ejecutar y desplegar los scripts	495
3.1 Por línea de comandos	495
3.2 Por GPO	496
3.2.1 Requisitos previos	497
3.2.2 Configurar la directiva de grupo	498
3.2.3 Implementar un filtro WMI	505
3.2.4 Vincular la directiva de grupo a un objeto	510
3.2.5 Comprobar la aplicación del objeto GPO en los puestos cliente	513
3.2.6 Desplegar y ejecutar un script una única vez	515
3.3 Uso de un archivo XML para sus scripts	516
3.3.1 Explicación y escenario de ejemplo	517
3.3.2 Datos encriptados en el archivo XML	520
Casos prácticos y otras características	
1. Conectar una unidad de red	523
2. Envío de e-mails	527
3. Implementar carpetas compartidas	531

Anexos

1. Lista de cmdlets	541
2. Lista de características disponibles en Windows 10	581
índice	585