

Ediciones ENI

Windows Server 2016

**Las bases imprescindibles
para administrar y configurar
su servidor**

(2ª edición)

Colección
Recursos Informáticos

Extracto del Libro

Capítulo 1

Roles y características

1. Organización del libro

El libro se compone de 18 capítulos, que presentan las distintas características del sistema operativo Windows Server 2016.

Con el objetivo de poder practicar en buenas condiciones, el capítulo Instalación del entorno de pruebas detalla la creación de una maqueta, equipada con 5 máquinas virtuales:

- **AD1, AD2, SV1 y SRVCore**, con Windows Server 2016.
- Una máquina cliente **CL10-01** con Windows 10.

Los capítulos, cada uno dedicado a un tema diferente, pueden recorrerse de manera independiente. Cada capítulo está construido para que pueda conocer la teoría y también su puesta en práctica sobre una o varias VM (o máquina virtual). El sistema operativo instalado en la máquina host es Windows Server 2012 R2, las máquinas virtuales funcionan con Windows Server 2016 en el caso de máquinas servidoras y con Windows 10 en la máquina cliente. AD1, AD2 y SV1 ejecutan su sistema operativo con una interfaz gráfica, SRVCore lo hace únicamente por línea de comandos.

Es posible descargar varios scripts y modelos de administración con formato ADM desde la página del libro en el sitio web de Ediciones ENI.

2. Roles

Los siguientes roles y características son una pequeña lista de aquellos presentes en Windows Server 2016.

Desde Windows Server 2008 R2, es posible instalar los distintos roles desde la consola **Administración del servidor**. Estos últimos aportan características suplementarias a los servidores. De este modo, el equipo IT puede ofrecer servicios suplementarios (direccionamiento IP automático de los puestos de trabajo y otro equipamiento conectado a la red, servidores de impresión...) a sus usuarios. La mayor parte de ellos contienen servicios de rol, que permiten habilitar ciertas funcionalidades. Se instalan bien generalmente durante la instalación de algún otro rol o funcionalidad. También pueden agregarse tras la instalación.

2.1 Acceso remoto

El rol **Acceso remoto** permite proveer un **servicio** VPN. La parte de enrutamiento está, también, presente y ofrece la funcionalidad que permite el enrutamiento de paquetes.

Los servicios de rol disponibles son:

- **Direct Access y VPN**: Direct Access permite establecer una conexión a la red de la empresa sin intervención alguna del usuario. La conexión se establece únicamente cuando el usuario se conecta desde el exterior de la red local.
- **Enrutamiento**: este servicio de rol permite instalar varios tipos de routers, entre ellos los que ejecutan RIP y los proxys IGMP.

2.2 Hyper-V

Desde Windows Server 2008, es posible instalar el hipervisor de Microsoft, **Hyper-V**. Permite implementar una plataforma de virtualización. Se ha enriquecido con Windows Server 2012 y 2012 R2. Se han integrado nuevas características a Windows Server 2016. Ahora es posible agregar en caliente para una VM una tarjeta de red virtual, así como la memoria. Esta funcionalidad resulta muy interesante y permite reducir el tiempo de indisponibilidad del servicio ofrecido por la máquina virtual correspondiente. Se han agregado otras funcionalidades, como la distribución del servicio de integración, a Hyper-V en Windows Server 2016.

2.3 DHCP (Dynamic Host Configuration Protocol)

El rol permite distribuir contratos DHCP a los distintos equipos que realizan la demanda. Puede instalarse sobre un servidor en modo instalación completa o en modo Core (instalación sin interfaz gráfica).

2.4 DNS (Domain Name System)

Obligatorio en un dominio Active Directory, permite resolver nombres en direcciones IP y a la inversa. Este servicio permite a su vez a los puestos cliente encontrar sus controladores de dominio. Puede instalarse sobre un servidor que no posea interfaz gráfica.

2.5 IIS (Internet Information Services)

Servidor web, permite mostrar y almacenar sitios y aplicaciones web. En la actualidad, cada vez es más frecuente que una aplicación posea una interfaz web.

Este rol es el que más servicios de rol posee.

- **Características HTTP comunes:** instala y administra las características HTTP básicas. Este servicio de rol permite crear mensajes de error personalizados con el objetivo de gestionar las respuestas generadas por el servidor.
- **Estado y diagnóstico:** aporta herramientas necesarias para la supervisión y el diagnóstico de la integridad de los servidores.
- **Rendimiento:** permite realizar compresión de contenido.
- **Seguridad:** implementa herramientas que permiten asegurar la seguridad del servidor frente a usuarios malintencionados y las consultas IIS.
- **Herramientas de administración:** provee herramientas de administración para las versiones anteriores de IIS.
- **Servidor FTP:** permite instalar y administrar un servidor FTP.

2.6 AD DS (Active Directory Domain Services)

Permite almacenar información de identificación de usuarios y equipos del dominio. Este rol se ejecuta en un servidor con el nombre del controlador de dominio, que tiene como función autenticar a los usuarios y los equipos presentes en el dominio AD.

Este rol puede instalarse en un servidor que no posea interfaz gráfica.

2.7 AD FS (Active Directory Federation Services)

El rol provee un servicio federado de gestión de identidades. Identifica y autentifica un usuario que quiera acceder a una extranet.

De este modo, dos empresas pueden compartir de forma segura información de identidad de Active Directory sobre un usuario Office 365 solo.

El rol está compuesto por varios servicios:

- **Servicio de federación:** instala la infraestructura necesaria para proveer acceso a los recursos.
- **Agente Web AD FS:** permite validar los testigos de seguridad entregados y autorizar un acceso autenticado a un recurso web.
- **Proxy FSP** - (*Federation Service Proxy*): permite recoger información de autenticación desde un navegador o una página web.

2.8 AD RMS (Active Directory Rights Management Services)

Protege un recurso contra un uso no autorizado. Los usuarios se identifican y se les concede permisos para acceder a la información protegida.

Es, así, más sencillo prohibir a un usuario copiar un documento en una memoria USB o imprimir un archivo confidencial.

Durante la instalación del rol, es posible instalar dos servicios:

- **Active Directory Rights Management Server:** permite proteger un recurso frente a un uso no autorizado.
- **Compatibilidad con la federación de identidades:** aprovecha las relaciones de federación entre dos organizaciones para establecer la identidad del usuario y permitirle el acceso a un recurso compartido.

2.9 AD CS (Active Directory Certificate Service)

Instala una autoridad de certificación con el objetivo de realizar operaciones de emisión y de administración de certificados.

Es posible agregar seis servicios de rol durante la instalación:

- **Autoridades de certificación:** provee una infraestructura de clave pública.
- **Inscripción en web de entidades de certificación:** se instala una interfaz web que permite, a un usuario, realizar solicitudes y renovaciones de certificados. Es, también, posible recuperar listas de revocación de certificados o realizar una inscripción de certificados de tarjetas.

- **Respondedor en línea:** permite gestionar y administrar la información del estado de la revocación.
- **Servicio de inscripción de dispositivos de red:** emite y gestiona los certificados de los routers y demás periféricos de red.
- **Servicio web de inscripción de certificados:** este servicio de rol ofrece la posibilidad a los usuarios y equipos de realizar la inscripción y renovación de certificados.
- **Servicio web de directiva de inscripción de certificados:** ofrece a los usuarios y equipos información sobre la directiva de inscripción de certificados.

2.10 Servicios de implementación de Windows (Windows Deployment Services - WDS)

Este rol provee un servicio de despliegue de sistemas operativos a través de la red. El servidor posee dos tipos de imágenes: **imágenes de arranque**, que permiten acceder a la instalación de Windows o a una carpeta compartida (MDT), e **imágenes de instalación**, que contienen los metadatos necesarios para la instalación del sistema operativo.

Con la instalación de este servicio es posible instalar dos servicios de rol:

- **Servidor de despliegue:** provee las funcionalidades necesarias para el despliegue de un sistema operativo. Este servicio también tiene en cuenta funcionalidades de captura.
- **Servidor de transporte:** se utiliza para transmitir datos en modo multidifusión.

2.11 Servicio de acceso y directivas de redes

Este rol permite gestionar accesos a la red mediante acceso inalámbrico, servidores VPN, así como conmutadores de autenticación 802.1x. La instalación de NPS (*Network Policy Server*) permite implementar la protección de acceso a la red (NAP).

Los servicios de rol disponibles son:

- **Servidor NPS:** permite implementar directivas de acceso a la red para las solicitudes de conexión.
- **Autoridad HRA:** emisión de certificados de integridad para los puestos de trabajo conforme a las exigencias de integridad.
- **HCAP** (*Host Credential Authorization Protocol*): la solución NAP está integrada con la solución de control de acceso Cisco.

2.12 WSUS

Permite aprobar las actualizaciones antes de su instalación en un puesto cliente, estando este último en un rango dentro de un grupo de ordenadores. Esta solución permite realizar una aprobación para un grupo en particular (por ejemplo: grupo "pruebas" en primer lugar y, a continuación, si el correctivo no provoca ningún problema, se aprueba para el resto).

Existen tres servicios de rol disponibles:

- **WID Database:** instala la base de datos que utiliza WSUS en WID (*Windows Internal Database*). Este tipo de base de datos pueden utilizarla otros roles (AD RMS, etc.).
- **WSUS Services:** instala el servicio WSUS, así como el resto de los componentes necesarios.
- **Base de datos:** instala la base de datos para los servicios WSUS (se necesita un servidor SQL, a diferencia de WID Database).

2.13 Servicios de archivos e iSCSI

El servicio de archivos permite implementar cuotas en el sistema de archivos, así como un sistema de filtrado por extensión, con el objetivo de prohibir que se almacenen ciertos archivos. Es posible instalar un espacio de nombres DFS mediante un servicio de rol.

Los siguientes servicios ofrecen la posibilidad de instalarse como servicio de rol:

- **Servidor de archivos:** gestión de carpetas compartidas.
- **BranchCache para archivos de red:** incluye BranchCache en el servidor. Este servicio permite implementar la caché de documentos con el objetivo de reducir el uso de la línea existente entre dos sitios remotos. El usuario solo tiene, por ejemplo, que buscar los documentos en su puesto local, de modo que se actualizan en caché en un servidor o un puesto local.
- **Desduplicación de datos:** permite liberar el espacio de disco suprimiendo datos duplicados; en el volumen se almacena una copia única de los datos idénticos.
- **Espacio de nombres DFS:** instala las herramientas necesarias para la creación y la gestión del espacio de nombres.
- **Administrador de recursos del servidor de archivos:** herramienta que permite administrar un sistema de archivos mediante la creación de cuotas y el filtrado de archivos.
- **Replicación DFS:** sincroniza carpetas sobre varios servidores locales o un sitio remoto.

Ediciones ENI

PowerShell Core y Windows PowerShell

Los fundamentos del lenguaje

(2ª edición)

Colección
Expert IT

Extracto del Libro

Capítulo 12 Seguridad

1. La seguridad: ¿para quién? ¿Por qué?

La aparición de las redes locales y de Internet ha cambiado muchas cosas en la manera de proteger su PC. Ya no basta con encadenar el disco duro a la mesa y cerrar la puerta del despacho por la noche para que no le roben o pirateen sus datos. Ahora, proteger su puesto de trabajo se ha convertido en algo esencial para no tener que remediar intrusiones o malas intenciones.

Pero entonces ¿contra quién prevenir? Pues contra todo lo que se mueve... y también los que no se mueven. En efecto, ya sean programas malintencionados, usuarios con malas intenciones, o hasta usuarios novatos, todos están considerados una amenaza. Por este motivo debe asegurar su sistema estableciendo reglas de seguridad, aplicándolas y asegurándose de que los demás hacen lo mismo.

2. Los riesgos vinculados al scripting

Adivinará rápidamente que lo que hace la fuerza del scripting se convierte en su debilidad. La facilidad con la que puede hacer todo, ya sea haciendo clic en un script o ejecutándolo desde la ventana de comandos, puede meterle en problemas si no presta atención.

Imagine un script de inicio de sesión que en la apertura de la sesión la bloquea enseguida! Claro, es divertido entre amigos, pero en una empresa, dudamos que esto sea bueno. Todavía peor un script de una persona malintencionada o realmente novata en PowerShell (en este caso, le aconsejamos comprarle un ejemplar de este libro...) puede perfectamente bloquear cuentas de usuarios en Active Directory, formatear el disco, reiniciar el sistema en un bucle infinito... Lo ha entendido, un script puede hacer de todo. Aunque a día de hoy se notifica al usuario con alertas para prevenirle de la ejecución de un script, estas no son capaces de determinar si un script es nocivo para el correcto funcionamiento del sistema.

Los riesgos vinculados al scripting se resumen a una historia de compromisos: o bien impide toda ejecución de scripts, es decir asumir el riesgo de «amargarle la vida» teniendo que hacer y rehacer tareas básicas y muy ingratas, o bien elige abrir su sistema a PowerShell, teniendo cuidado de tomar las precauciones que se imponen.

Pero no se deje desanimar ya que aunque la ejecución de scripts le expone a ciertos problemas de seguridad, PowerShell está dotado de ciertos conceptos que hacen de él uno de los lenguajes de script más seguros. No hay que olvidar que en caso de problemas de seguridad, es la imagen de Microsoft en su conjunto la que sufre...

3. Optimizar la seguridad de PowerShell

3.1 La seguridad de PowerShell por defecto

Lo ha entendido, la seguridad es una área muy importante, sobre todo en el dominio del scripting. Por este motivo los creadores de PowerShell han incluido dos reglas de seguridad por defecto.

Los archivos ps1 asociados al bloc de notas

La extensión «.ps1» de los scripts PowerShell está por defecto asociada al bloc de notas (o Notepad). Este procedimiento permite evitar ejecutar automáticamente scripts potencialmente peligrosos por una mala manipulación. El bloc de notas es, realmente, un editor un poco clásico, pero tiene la doble ventaja de ser inofensivo y de no bloquear la ejecución de un script cuando este está abierto con el editor. Observará sin embargo que la edición (clic con el botón derecho + **Modificar**) de archivos .ps1 está asociada al editor ISE.

■ Observación

Este tipo de seguridad no existía con los scripts VBS cuya apertura estaba directamente asociada a Windows Script Host.

Una directiva de ejecución restringida

La segunda barrera de seguridad es la aplicación de la directiva de ejecución **Restricted** por defecto para los puestos clientes y **RemoteSigned** por defecto para los servidores (desde Windows Server 2012 R2).

La directiva **Restricted** es la más restrictiva. Es decir que bloquea sistemáticamente la ejecución de todos los scripts. Solo se ejecutan los comandos tecleados en la shell. Para remediar a esta situación, PowerShell requiere que el usuario cambie el modo de ejecución con el comando **Set-ExecutionPolicy <modo de ejecución>**. Pero para ello debe ser administrador del equipo.

■ Observación

Igual comprende mejor por qué el uso de PowerShell en sus equipos no constituye un aumento del riesgo, en la medida en que se respetan ciertas reglas.

3.2 Las directivas de ejecución

PowerShell integra un concepto de seguridad que llamamos directivas de ejecución (execution policies) para que un script no autorizado no pueda ejecutarse en contra de la voluntad del usuario. Existen siete configuraciones posibles: **Restricted**, **RemoteSigned**, **AllSigned**, **UnRestricted**, **Bypass**, **Default** y **Undefined**. A cada una de ellas le corresponde un nivel de autorización de ejecución de determinados scripts. Podrá llegar a cambiar en función de la directiva que desee aplicar.

3.2.1 Las diferentes directivas de ejecución

Restricted: es la directiva más restrictiva y también la directiva por defecto en los puestos cliente (de Windows 7 a Windows 10). No permite la ejecución de scripts pero autoriza las instrucciones por la línea de comandos tecleadas en la consola (modo interactivo). Esta directiva puede considerarse como la más radical dado que protege frente a la ejecución de archivos **.ps1**.

Con esta directiva, al tratar de ejecutar un script, se muestra un mensaje de este tipo en la consola:

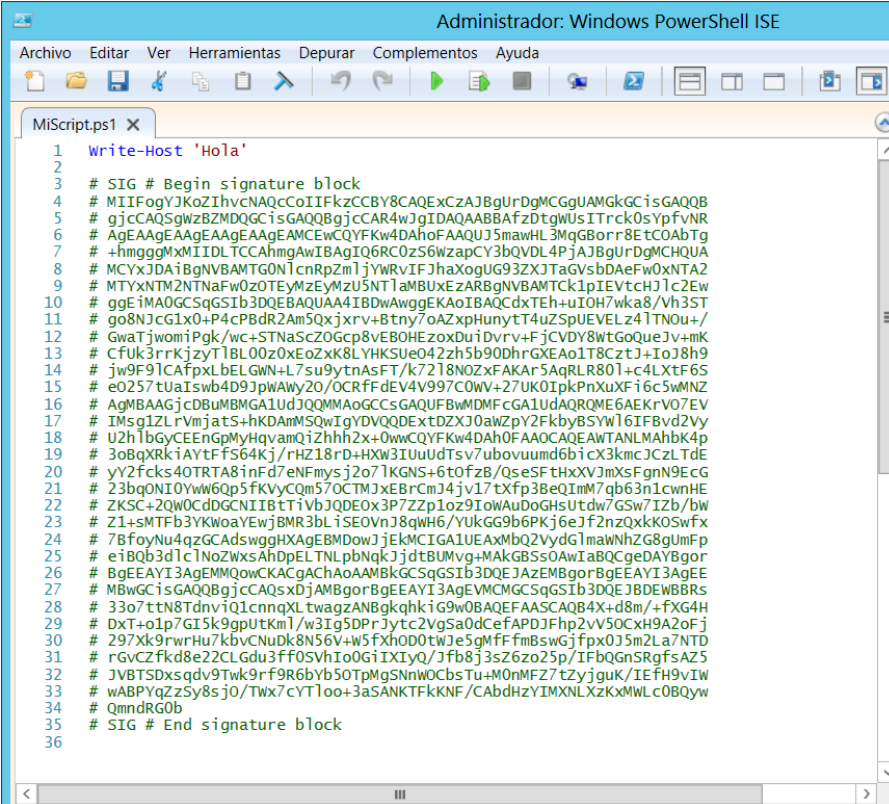
```
.\lanzadera.ps1 : File C:\temp\lanzadera.ps1 cannot be loaded because running
scripts is disabled on this system. For more information, see
about_Execution_Policies at https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1 *
+ .\lanzadera.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
```

Si esta es la directiva definida por defecto en la instalación de PowerShell, tendrá que cambiarla para la ejecución de su primer script.

Observación

Para poder modificar la directiva de ejecución PowerShell, deberá ser administrador local de la máquina.

AllSigned: es la directiva más «segura» que permite la ejecución de scripts. Autoriza únicamente la ejecución de scripts firmados. Un script firmado es un script que contiene una firma digital como la que se muestra en la figura de abajo.



```

Administrador: Windows PowerShell ISE
Archivo  Editar  Ver  Herramientas  Depurar  Complementos  Ayuda

MiScript.ps1 x
1  write-Host 'Hola'
2
3  # SIG # Begin signature block
4  # MIIIFogYJKozIhvcNAQcCoIIFkzCCBY8CAQeCzAJBgUrDgMCGGUAMGkGcisGAQQB
5  # gjcCAQSwgBZMDQGCisGAQQBgjcCAR4wJgIDAQAABAFzDgUuSITrck0sYpFvNR
6  # AgEAAgEAAGAAgEAAGAAgEAACEwCQYFk4DAHoFAAQUJ5mawHL3MqGBorr8EtCoAbTg
7  # +hmgggMxMIIDLTCcAHmgAwIBAgIQ6RC0zS6wzapCY3bQVLD4PjAJBgUrDgMCHQUA
8  # MCYxJDAiBgnVBAMTGNlcnRpZmljYWRvIFJhaXogUG93ZXJTaGvsbDAAEw0xNTA2
9  # MTYxNTM2NTNfaW0zOTEmZmZlYmZlNTlaMBUxEzARBgNVBAMTck1pIEVtCHJlC2Ew
10 # ggEiMA0GCsGSIb3DQGEBAQUAA4IBDwAwgGEKAoIBAQCdxTEh+uIOH7wka8/Vh3ST
11 # go8NjCGlX0+P4cPBR2Am5Qxjxrv+BtNy7oAZxpHunyT4uZSpUEVELZ41TNUou+/
12 # GwaTjwomiPgk/wc+STNaSc2OGcp8vEBOHEzoxDuiDvrv+fjCVDY8wtGoQueJv+mK
13 # CfUk3rrkjzyTlBL00z0xEozxk8LYHKSUE042h590DhrGXEAo1T8CztJ+IoJ89
14 # jw9F9tCAfpxlBELGWN+L7su9ytnAsFT/k7218N0zxfAKAr5AqRLR801+c4LXTF6S
15 # e0257tUaIswb4D9jpwAwY20/OCrFFdeV4V997COWv+27UK0iPknXuxF16c5wMNZ
16 # AgMBAAGjCDBuMBMGA1UdJQcMMoGCSsGAQUFBwMDMFCGAlUdAQRQME6AEKrv07EV
17 # ImSg1ZLrVmjt+s+hKdAmMSQwIgyDVQqDExtDZXJ0awZpY2FkbyBSYwI6IFBvd2Vy
18 # U2h1bGyCEENgpMyHqyAmQiZihh2x+0wwCQYFk4DAHoFAAOCAQEAwTANLMAhK4p
19 # 3oBqXRk1AYTF564Kj/rHZ18rD+HXW3IUuUdTs7ubovuumd6bi cX3kmcJcZLTde
20 # yY2fcks40RTA8InFd7eNfmysj2o71KGNS+6t0fzB/QseSFtHxxVJmXsFgnN9EcG
21 # 23bqONI0Yww6qp5fKvYcQm570CTMJxEBrCmJ4jv17tXfp3BeQImM7qb63n1cwnHE
22 # ZK5C+2Qw0cDdGNCiIBtTiVbJQDE0x3P7ZzP1oz9IowAudoGhsUtdw/Gsw7IZb/bw
23 # Z1+sMTFb3YKwoaYewjBMR3bLiSE0VnJ8qWH6/YukGG9b6PKj6eJf2nzQxkko5wfx
24 # 7Bfoynu4qzGcAdswggHXAgEBMDowJjEkMCIgA1UEAxMBQ2Vydg1mawNhZG8GUmFp
25 # eiBQb3d1c1NoZwxsAhDpELTNLpbNqkJjdtBUMvg+MAKGBS0AwIaBQCgeDAYBgor
26 # BgEEAYI3AgEMMQowKcACgAChAoAAMBgkCgSgSIb3DQEAJzEMBgorBgEEAYI3AgEE
27 # MBWGCisGAQQBgjcCAQsxDjAMBgorBgEEAYI3AgEVMCMGCSgSIb3DQEJBDEWBBS
28 # 3307tN8Tdnv1Q1cnnqXLtwagzANBqkqhkiG9w0BAQEFAASCAQBA4+d8m/+fXG4H
29 # Dxt+o1p7GI5k9gpUtKml/w3Ig5DPrytc2VgSa0dCefAPDJFhp2vV50cxH9A2ofJ
30 # 297Xk9rwrHu7kbvCNUdK8N56v+w5fxh0D0twJe5gmFFfmbSwgJfpx0J5m2La7NTD
31 # rGVCzFkd8e22CLGdu3ff0SvHio0GiIXiyQ/JfB8j3sz6zo25p/IFbQGNsRgfsAZ5
32 # JVBTSdxsQdv9Tkw9rF9R6bYb50TpmgSnnwOCbsTu+M0nMFZ7tzyguK/IEFh9vIW
33 # wABPYqzZSy8sJ/Twx7cYT1oo+3aSANKTFKKNF/CABdhZYIMXNLXzXkMWLCOBQyw
34 # QmndRG0b
35 # SIG # End signature block
36

```

Ejemplo de script firmado

Con la directiva **AllSigned**, la ejecución de scripts firmados necesita que esté en posesión de los certificados correspondientes (consulte la sección Firma de scripts).

RemoteSigned: esta directiva es similar a **AllSigned** con la diferencia de que solo los scripts que tienen un origen distinto al local necesitan una firma. Por consiguiente, todos sus scripts creados localmente pueden ser ejecutados sin necesidad de firma.

A partir de Windows Server 2012 R2, PowerShell se ejecuta con esta directiva de ejecución por defecto, lo que no era el caso en las versiones anteriores de Windows Server.

Si intenta ejecutar un script descargado de Internet sin estar firmado, obtendrá el siguiente mensaje de error.

```
.\Get-Script.ps1: File C:\Temp\Script.ps1 cannot be loaded.  
The file C:\Temp\Script.ps1 is not digitally signed.
```

Observación

Seguramente se pregunte ¿cómo hace PowerShell para saber que nuestro script tiene su origen en Internet? Respuesta: Gracias a los «Alternate Data Streams» que se implementan con la forma de flujos cachés desde las aplicaciones de comunicación tales como Microsoft Outlook, Internet Explorer, Outlook Express y Windows Messenger (consulte la sección dedicada a los Alternate Data Streams). En resumen, cuando descarga un script desde un cliente Microsoft, se le adjunta su origen.

Unrestricted: con esta directiva todos los scripts, sea cual sea su origen, se ejecutan sin solicitar una firma.

Esta directiva muestra aun así un aviso cuando intenta ejecutar algún script descargado de Internet.

```
PS > .\script.ps1
```

```
Security warning
```

```
Run only scripts that you trust. While scripts from the internet can  
be useful, this script can potentially harm your computer. If you trust  
this script, use the Unblock-File cmdlet to allow the script to run  
without this warning message. Do you want to run C:\Temp\script.ps1?  
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"):
```

Bypass: es la directiva menos restrictiva, y por lo tanto la menos segura. No se bloquea nada y no se muestra ningún mensaje de aviso. Es por lo tanto la directiva con el riesgo más elevado de ejecutar scripts malintencionados.

Undefined: no se ha definido ninguna directiva para el ámbito actual. Si no se definen directivas de ejecución en ningún ámbito entonces la directiva efectiva será la directiva **Restricted**.

Default: carga la directiva por defecto, a saber **Restricted**.

■ Observación

Microsoft ha puesto en marcha mecanismos con el fin de intentar limitar los riesgos vinculados a la ejecución de scripts que provengan del exterior de la empresa y por lo tanto potencialmente peligrosos. La configuración por defecto permite alcanzar este objetivo pero no garantiza en ningún caso una seguridad perfecta.

3.2.2 Los ámbitos de las directivas de ejecución

PowerShell permite gestionar el ámbito de las directivas. El orden de aplicación es el siguiente:

- **Ámbito Process**: la directiva de ejecución solo afecta a la sesión actual (proceso Windows PowerShell). El valor asignado al ámbito **Process** se almacena únicamente en memoria; por lo tanto no se conserva al cerrar la sesión de PowerShell.
- **Ámbito CurrentUser**: la directiva de ejecución aplicada al ámbito **CurrentUser** solo afecta al usuario actual. Se almacena el tipo de directiva de manera permanente dentro de la clave de registro **HKEY_CURRENT_USER**.
- **Ámbito LocalMachine**: la directiva de ejecución aplicada al ámbito **LocalMachine** afecta a todos los usuarios del equipo. Se almacena el tipo de directiva de manera permanente dentro de la clave de registro **HKEY_LOCAL_MACHINE**.

La directiva con prioridad 1 tiene preferencia sobre la que tenga prioridad 3. Por lo tanto si el ámbito **LocalMachine** es más restrictivo que el ámbito **Process**, la directiva aplicada será aun así la del ámbito **Undefined** en cuyo caso PowerShell aplicará la directiva del ámbito **CurrentUser** y después intentará aplicar la directiva **LocalMachine**.

Recuerde que el ámbito **LocalMachine** es el definido por defecto cuando aplicamos una directiva de ejecución sin precisar un ámbito particular.

3.2.3 Identificar la directiva de ejecución actual

La directiva de ejecución actual se obtiene con el comando **Get-ExecutionPolicy**.

Ejemplo

```
PS > Get-ExecutionPolicy
Restricted
```

Con este comando, tenemos la opción **-List**. Gracias a ella, sabremos qué directivas se aplican en cada ámbito.