

Para ver el artículo en inglés, active la casilla Inglés. También puede ver el texto en inglés en una ventana emergente si pasa el puntero del mouse por el texto.

# Herramientas de seguridad para administrar Windows Server 2012

Se aplica a: Windows Server 2012, Windows 8

En este tema destinado a los profesionales de TI, se enumeran y describen las herramientas de Microsoft disponibles para Windows Server 2012 que permiten administrar tecnologías de seguridad y enfrentar amenazas continuas en equipos y redes.

Para que le resulte más fácil encontrar la herramienta indicada para el trabajo, las siguientes herramientas de seguridad están agrupadas por categoría y tarea:

Categoría	Tarea
Acceso	<a href="#">Administrar el acceso a los recursos de red</a>
Auditoría	<a href="#">Administrar el acceso a los recursos de red</a>
Servicios de certificados	<a href="#">Administrar una CA y otras tareas de Servicios de certificados de Active Directory</a>
Equipo	<a href="#">Analizar y administrar el rendimiento y los procesos del equipo</a>

Credenciales	<a href="#">Administrar credenciales, grupos y cuentas de usuario</a>
Criptografía	<a href="#">Administrar certificados y cifrado</a>
Archivos	<a href="#">Tomar posesión de los archivos o eliminarlos de forma segura</a>
Directivas de seguridad	<a href="#">Analizar y administrar directivas de seguridad</a>
Entidades de seguridad	<a href="#">Modificar o crear nuevas entidades de seguridad</a>
Seguridad del sistema	<a href="#">Diagnosticar, planear y corregir la seguridad general del sistema</a>

En la lista siguiente se ofrecen vínculos a los cmdlets de seguridad incluidos en los módulos principales de Windows PowerShell y vínculos a los cmdlets de tecnologías que se usan en ocasiones para administrar la seguridad de su empresa.

- [Windows PowerShell Security Cmdlets](#)
- [PowerShell Cmdlets for Active Directory](#)
- [PowerShell Cmdlets for Active Directory Rights Management Services](#)
- [PowerShell Cmdlets for Applocker](#)
- [PowerShell Cmdlets for Group Policy](#)
- [PowerShell Cmdlets for Server Manager](#)
- [PowerShell Cmdlets for the Best Practice Analyzer](#)
- [Script Center Gallery](#)

# Administrar credenciales, grupos y cuentas de usuario

La administración de identidades de usuario y los procesos de inicio de sesión y autenticación implican tareas importantes, aunque a menudo repetitivas. Para obtener información relacionada y administrar credenciales, grupos y cuentas de usuario, use una de las herramientas siguientes.


Herramienta	Tipo	Descripción
<a href="#">Whoami [LH]</a>	Herramienta de línea de comandos de Windows	Muestra información del usuario, el grupo y los privilegios del usuario que tiene una sesión iniciada actualmente en el equipo local. Si se usa sin parámetros, <b>whoami</b> muestra el nombre de usuario y el dominio actuales.
<a href="#">Cmdkey [LH]</a>	Herramienta de línea de comandos de Windows	Crea, enumera y elimina los nombres de usuario y las contraseñas o credenciales almacenados.
<a href="#">Net localgroup [LH]</a>	Herramienta de línea de comandos de Windows	Agrega, muestra o modifica grupos locales.
<a href="#">Net user [LH]</a>	Herramienta de línea de comandos de Windows	Agrega o modifica cuentas de usuario o muestra información de la cuenta de usuario.
<a href="#">Get-Credential</a>	Cmdlet de Windows	Obtiene un objeto de credencial basado en un nombre de usuario

	PowerShell	y una contraseña.
<a href="#">Get-Authenticode Signature</a>	Cmdlet de Windows PowerShell	Obtiene información sobre la firma Authenticode en un archivo.
<a href="#">LogonSessions</a>	Utilidad de Sysinternals	Enumera las sesiones de inicio activas.
<a href="#">PsLoggedOn</a>	Utilidad de Sysinternals	Muestra los usuarios que tienen una sesión iniciada en un equipo.

## Modificar o crear nuevas entidades de seguridad

Agregar, eliminar y modificar la información de cuenta y de grupo es una de las tareas de administrador más frecuentes. Para modificar o crear nuevas entidades de seguridad, use una de las herramientas siguientes.

Herramienta	Tipo	Descripción
<a href="#">Ktpass [LH]</a>	Herramienta de línea de comandos de Windows	Configura el nombre de la entidad de seguridad del servidor para el host o servicio en los Servicios de dominio de Active Directory (AD DS) y genera un archivo .keytab que contiene la clave secreta compartida del servicio.

		<div>  <b>Nota</b> </div> <p>El archivo .keytab se basa en la implementación del Instituto Tecnológico de Massachusetts (MIT) del protocolo de autenticación Kerberos. La herramienta de línea de comandos Ktpass permite a los servicios basados en UNIX que admiten la autenticación Kerberos usar las características de interoperabilidad proporcionadas por el servicio Centro de distribución de claves (KDC) en Windows Server 2008.</p>
<a href="#">Cmdkey [LH]</a>	Herramienta de línea de comandos de Windows	Crea, enumera y elimina los nombres de usuario y las contraseñas o credenciales almacenados.
<a href="#">Net localgroup [LH]</a>	Herramienta de línea de comandos de Windows	Agrega, muestra o modifica grupos locales.
<a href="#">Net user [LH]</a>	Herramienta de línea de comandos de Windows	Agrega o modifica cuentas de usuario o muestra información de la cuenta de usuario.

<a href="#">Dsadd [LH]</a>	Herramienta de línea de comandos de Windows	Permite agregar tipos de objetos específicos al directorio.
<a href="#">Add-Computer</a>	Cmdlet de Windows PowerShell	Agrega equipos a un dominio o grupo de trabajo.
<a href="#">Remove-Computer</a>	Cmdlet de Windows PowerShell	Quita los equipos de grupos de trabajo o dominios.
<a href="#">Reset-ComputerMachinePassword</a>	Cmdlet de Windows PowerShell	Restablece la contraseña de la cuenta de equipo.

## Administrar certificados y cifrado

Los certificados y el cifrado pueden reforzar en gran medida la seguridad de una red y sus recursos. Para administrar las solicitudes de certificados y los directorios o archivos cifrados, use las siguientes herramientas.

Herramienta	Tipo	Descripción
<a href="#">CertReq [WS2012]</a>	Herramienta de línea de comandos de Windows	Solicita certificados de una entidad de certificación (CA), recupera una respuesta a una solicitud anterior de una CA, crea una nueva solicitud a partir de un archivo .inf, acepta e instala una respuesta a una solicitud, crea una solicitud de certificación cruzada o de subordinación completa a partir de una solicitud o un certificado de

		CA existente o inicia una solicitud de certificación cruzada o de subordinación completa.
Cifrado	Herramienta de línea de comandos de Windows	Muestra o cambia el cifrado de directorios y archivos en volúmenes NTFS. Si se utiliza sin parámetros, <b>cipher</b> muestra el estado de cifrado del directorio actual y los archivos que contiene.
Get-PfxCertificate	Cmdlet de Windows PowerShell	Obtiene información sobre archivos de certificado .pfx en el equipo.
Proveedor de certificados	Proveedor de Windows PowerShell	Permite navegar por el espacio de nombres de certificado y ver los almacenes de certificados y los certificados. También puede copiar, mover y eliminar certificados y almacenes de certificados, así como abrir el complemento Certificados de Microsoft Management Console (MMC).

## Administrar una CA y otras tareas de Servicios de certificados de Active Directory

Los Servicios de certificados de Active Directory (AD CS) permiten a una organización emitir y administrar certificados que habilitan varios requisitos de infraestructura de red. Para administrar una CA y completar otras tareas de AD CS, use la herramienta siguiente.

Herramienta	Tipo	Descripción
<a href="#">Certutil [W2012]</a>	Herramienta de línea de comandos de Windows	Recopila y muestra la información de configuración de la entidad de certificación (CA), configura AD CS, realiza copias de seguridad y restaura los componentes de la CA y comprueba los certificados, los pares de claves y las rutas de certificación.

## Administrar el acceso a los recursos de red

Los archivos, las carpetas y los recursos compartidos que están protegidos mediante listas de control de acceso (ACL) se pueden supervisar y administrar con las herramientas, los cmdlets y las utilidades siguientes. Para obtener información sobre los permisos de acceso de los recursos, utilice una de las siguientes herramientas.

Herramienta	Tipo	Descripción
<a href="#">Icacs [LH]</a>	Herramienta de línea de comandos de Windows	Muestra o modifica las listas de control de acceso discrecional (DACL) en los archivos especificados y aplica las DACL almacenadas a los archivos de los directorios especificados. Icacs.exe reemplaza a la herramienta Cacs.exe para la visualización y edición de DACL.
<a href="#">Dscls [LH]</a>	Herramienta de línea de comandos de Windows	Muestra y cambia los permisos (entradas de control de acceso) en la ACL de objetos de Servicios de dominio de Active Directory (AD DS).



<a href="#">Get-Acl</a>	Cmdlet de Windows PowerShell	Obtiene el descriptor de seguridad de un recurso, como una clave del Registro o archivo.
<a href="#">ShareEnum</a>	Utilidad de Sysinternals	Permite examinar los recursos compartidos de archivos en la red y ver su configuración de seguridad.
<a href="#">AccessChk</a>	Utilidad de Sysinternals	Muestra los permisos de acceso a archivos, claves del Registro o servicios de Windows de un usuario o grupo especificado.
<a href="#">AccessEnum</a>	Utilidad de Sysinternals	Muestra los permisos de acceso a directorios, archivos y claves del Registro de todos los usuarios y grupos en los equipos de su dominio.

## Tomar posesión de los archivos o eliminarlos de forma segura

Los administradores pueden necesitar modificar la propiedad de los archivos o asegurarse de que no es posible acceder a los archivos eliminados. Para tomar posesión de los archivos o eliminarlos de forma segura, utilice una de las herramientas siguientes.

Herramienta	Tipo	Descripción
<a href="#">Takeown [LH]</a>	Herramienta de línea de comandos de Windows	Permite que un administrador recupere el acceso a un archivo que anteriormente le era denegado, convirtiendo al administrador en el propietario del archivo.

<a href="#">SDelete</a>	Utilidad de Sysinternals	Permite sobrescribir los archivos confidenciales y quitar archivos eliminados anteriormente con seguridad mediante este programa de eliminación segura conforme con el Departamento de Defensa.
-------------------------	--------------------------	---

## Administrar auditorías de seguridad y registros de auditoría

Las auditorías de seguridad permiten supervisar y analizar una amplia variedad de actividades de red y del equipo. Las utilidades siguientes pueden utilizarse para configurar el registro de eventos y administrar los registros de eventos y sus entradas.

Herramienta	Tipo	Descripción
<a href="#">Auditpol [Vista]</a>	Herramienta de línea de comandos de Windows	Muestra información relacionada y realiza funciones para modificar la configuración de directiva de auditoría.
<a href="#">Logman [vista]</a>	Herramienta de línea de comandos de Windows	Crea y administra registros de rendimiento y de sesión de seguimiento de eventos, y admite muchas funciones del Monitor de rendimiento desde la línea de comandos.
<a href="#">Clear-EventLog</a>	Cmdlet de Windows PowerShell	Elimina todas las entradas de los registros de eventos especificados en un equipo local o remoto.
<a href="#">Get-Event</a>	Cmdlet de Windows	Obtiene los eventos de la cola de eventos.


	PowerShell	
<a href="#">Get-EventLog</a>	Cmdlet de Windows PowerShell	Obtiene los eventos de un registro de eventos especificado o una lista de los registros de eventos de un equipo.
<a href="#">New-Event</a>	Cmdlet de Windows PowerShell	Crea un evento.
<a href="#">New-EventLog</a>	Cmdlet de Windows PowerShell	Crea un registro de eventos y un origen de eventos en un equipo local o remoto.
<a href="#">Remove-event</a>	Cmdlet de Windows PowerShell	Elimina eventos de la cola de eventos.
<a href="#">Remove-EventLog</a>	Cmdlet de Windows PowerShell	Elimina un registro de eventos o anula el registro de un origen de eventos.
<a href="#">Show-EventLog</a>	Cmdlet de Windows PowerShell	Muestra los registros de eventos del equipo local o remoto en el Visor de eventos.
<a href="#">Write-EventLog</a>	Cmdlet de Windows PowerShell	Escribe un evento en un registro de eventos.
<a href="#">Limit-EventLog</a>	Cmdlet de Windows PowerShell	Establece las propiedades de registro de eventos que limitan el tamaño del registro de eventos y la antigüedad de sus entradas.
<a href="#">PsLogList</a>	Utilidad de Sysinternals	Permite recopilar registros de eventos.

<a href="#">Wevtutil [Vista]</a>	Herramienta de línea de comandos de Windows	Permite recuperar información acerca de los registros de eventos y los editores. También puede utilizar este comando para instalar y desinstalar los manifiestos de eventos, ejecutar consultas, y exportar, archivar y borrar registros.
----------------------------------	---	---

## Analizar y administrar directivas de seguridad

La directiva de seguridad es el conjunto configurable de reglas que sigue el sistema operativo a la hora de determinar los permisos que ha de conceder en respuesta a una solicitud de acceso a los recursos. Puede utilizar las siguientes herramientas para analizar y administrar la configuración de directiva de seguridad de un único equipo o un dominio.

Herramienta	Tipo	Descripción
<a href="#">Asistente para configuración de seguridad [w8]</a>	Herramienta administrativa de Windows	Determina la funcionalidad mínima necesaria para los roles de un servidor y deshabilita las funciones innecesarias.
<a href="#">Secedit [LH]</a>	Herramienta de línea de comandos de Windows	Configura y analiza la seguridad del sistema mediante la comparación de una configuración existente con al menos una plantilla.
<a href="#">GPUpdate</a>	Herramienta de línea de comandos de Windows	Actualiza la configuración de directiva de grupo local y de dominio, incluida la configuración de seguridad.

		<div>  <b>Nota</b> </div> <p>Esta herramienta de línea de comandos reemplaza la opción <b>/refreshpolicy</b> del comando <b>secedit</b>.</p>
<b>Gpresult [LH]</b>	Herramienta de línea de comandos de Windows	Muestra información del conjunto resultante de directivas (RSOP) de un usuario local o de dominio y un equipo.
Directiva de seguridad local	Complemento Microsoft Management Console (MMC)	El complemento Directiva de seguridad (secpol.msc) permite ajustar la configuración de directivas de cuenta, directivas locales, Firewall de Windows con seguridad avanzada, Directivas de Administrador de lista de redes, directivas de clave pública, directivas de restricción de software, directivas de control de aplicaciones, directivas de seguridad IP en equipo local y la configuración de directiva de auditoría avanzada.
Plantillas de seguridad	Complemento Microsoft Management Console (MMC)	Las plantillas de seguridad proporcionan configuración de seguridad estándar para usarla como modelo para las directivas de seguridad. Ayudan a solucionar problemas relacionados con los equipos cuya configuración de seguridad no cumpla con la directiva o sea desconocida. Las plantillas de seguridad están inactivas hasta que se importan en un objeto de directiva de grupo o el

		complemento Configuración y análisis de seguridad en MMC.
<a href="#">Información técnica de AppLocker</a>	Complemento Microsoft Management Console (MMC)	AppLocker ayuda a controlar las aplicaciones y los archivos que los usuarios pueden ejecutar. Éstos incluyen archivos ejecutables, scripts, archivos de Windows® Installer, DLL, aplicaciones empaquetadas e instaladores de tales aplicaciones. También puede usar AppLocker para aplicaciones de inventario que se ejecutan en sus equipos.
<a href="#">Información general de las directivas de restricción de software</a>	Complemento Microsoft Management Console (MMC)	Puede usar las directivas de restricción de software para crear una configuración muy restringida para los equipos, en los que solamente pueden ejecutarse aquellas aplicaciones específicamente identificadas. Las directivas de restricción de software están integradas en Microsoft Active Directory y la directiva de grupo. También puede crear directivas de restricción de software en equipos independientes. Las directivas de restricción de software son directivas de confianza, las cuáles son normativas establecidas por un administrador para restringir los scripts y otros códigos que no son de confianza plena.

## Analizar y administrar el rendimiento y los procesos del equipo

La comprensión de la configuración y el comportamiento de un equipo, así como de las aplicaciones y los procesos que se ejecutan en ese equipo, es importante para diagnosticar problemas de rendimiento y errores del sistema, pero puede requerir una investigación detallada. Las siguientes herramientas pueden ayudarle con muchas de estas tareas.

Herramienta	Tipo	Descripción
<a href="#">Runas [LH]</a>	Herramienta de línea de comandos de Windows	Permite a un usuario ejecutar herramientas y programas específicos con permisos diferentes a los del inicio de sesión del usuario actual.
<a href="#">Sc [Vista]</a>	Herramienta de línea de comandos de Windows	Se comunica con el controlador del servicio y los servicios instalados.
<a href="#">Shutdown [Vista]</a>	Herramienta de línea de comandos de Windows	Permite apagar o reiniciar los equipos locales o remotos de uno en uno.
<a href="#">Tasklist [LH]</a>	Herramienta de línea de comandos de Windows	Muestra una lista de procesos en ejecución actualmente en el equipo local o en un equipo remoto.
<a href="#">Taskkill [LH]</a>	Herramienta de línea de comandos de Windows	Finaliza uno o más procesos o tareas. Los procesos se pueden finalizar por el identificador del proceso o el nombre de la imagen.

<a href="#">Bootcfg [Vista]</a>	Herramienta de línea de comandos de Windows	Configura, consulta o cambia la configuración del archivo Boot.ini.
<a href="#">Get-ExecutionPolicy</a>	Cmdlet de Windows PowerShell	Obtiene las directivas de ejecución en la sesión actual.
<a href="#">Set-ExecutionPolicy</a>	Cmdlet de Windows PowerShell	Cambia la preferencia de usuario para la directiva de ejecución del shell.
<a href="#">ShellRunAs</a>	Utilidad de Sysinternals	Permite iniciar programas como un usuario diferente a través de una entrada de menú contextual de shell.
<a href="#">PsTools</a>	Utilidad de Sysinternals	Incluye herramientas de línea de comandos para la enumeración de los procesos que se ejecutan en equipos locales o remotos, la ejecución de procesos de forma remota, el reinicio de equipos y la obtención de copias de los registros de eventos.
<a href="#">Autologon</a>	Utilidad de Sysinternals	Permite omitir la pantalla de contraseña durante el inicio de sesión.
<a href="#">Autoruns</a>	Utilidad de Sysinternals	Muestra los programas que están configurados para iniciarse automáticamente cuando se inicia un equipo y el usuario inicia sesión. Autoruns también muestra las ubicaciones del Registro y los archivos donde las aplicaciones pueden configurar



		valores de inicio automático.
<a href="#">Process Explorer</a>	Utilidad de Sysinternals	Permite averiguar qué archivos, claves del Registro y otros procesos de objetos están abiertos, qué bibliotecas de vínculos dinámicos (DLL) han cargado y a quién pertenece cada proceso.
<a href="#">PsExec</a>	Utilidad de Sysinternals	Permite ejecutar procesos con derechos de usuario limitados.

## Diagnosticar, planear y corregir la seguridad general del sistema

Microsoft proporciona una serie de herramientas gratuitas que se pueden usar para diagnosticar el estado general del sistema, planear mejoras y migraciones, y proteger contra el riesgo de infección de malware. Las siguientes herramientas pueden usarse para realizar estas tareas.

Herramienta	Tipo	Descripción
<a href="#">Kit de inicio para desarrolladores de ciclo de vida de desarrollo de seguridad</a>	Descarga	El kit de inicio para desarrolladores de SDL ofrece 14 módulos de contenido (con notas del orador, guías de moderador y preguntas de comprensión de ejemplo), además de ocho laboratorios virtuales de MSDN con manuales de laboratorio, todo ello creado para compilar un programa de formación de SDL personalizado para los equipos de desarrollo.

<a href="#">Herramienta de eliminación de software malintencionado</a>	Descarga	Comprueba los equipos que ejecutan Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003 Windows 8, Windows 7, Windows Vista y Windows XP en busca de infecciones causadas por determinado software malintencionado prevalente y ayuda a quitar cualquier infección encontrada.
<a href="#">Microsoft Security Assessment Tool</a>	Descarga	Proporciona información y recomendaciones sobre las prácticas recomendadas para ayudar a mejorar la seguridad en la infraestructura de TI.
<a href="#">Enhanced Mitigation Experience Toolkit v4.0</a>	Descarga	Permite diseñar métodos de mitigación para ayudar a evitar que usuarios malintencionados obtengan acceso a su sistema.
<a href="#">Microsoft Threat Analysis &amp; Modeling Tool</a>	Descarga	Permite especificar información, incluidos los requisitos empresariales y la arquitectura de aplicaciones, que se usará para generar un modelo de amenazas.
RootkitRevealer	Utilidad de Sysinternals	Permite analizar el equipo en busca de malware basado en rootkit.
<a href="#">Sigcheck</a>	Utilidad de Sysinternals	Permite recopilar información de versión de archivo y comprobar que las imágenes en el equipo están firmadas digitalmente.
<a href="#">Attack Surface Analyzer</a>	Descarga	Permite catalogar los cambios realizados en la superficie de ataque

		del sistema operativo por la instalación de software nuevo.
<a href="#">Microsoft Assessment and Planning Toolkit</a>	Descarga	MAP Toolkit es una poderosa herramienta de inventario, evaluación e informes capaz de evaluar con seguridad entornos de TI de distintas migraciones de plataforma. Tener un inventario de las plataformas que existen en el entorno puede permitirle implementar actualizaciones de seguridad más rápidamente, reaccionar frente a incidentes de seguridad, contener los problemas que puedan surgir y recuperarse más rápidamente de dichos problemas.

## Vea también

En la tabla siguiente, se proporcionan recursos adicionales de herramientas de seguridad de tecnologías relacionadas.

<b>Group Policy</b>	<a href="#">Introducción a las directivas de grupo</a>
<b>Servicios de dominio de Active Directory</b>	<a href="#">Introducción a los Servicios de dominio de Active Directory</a>
<b>Servicios de certificados de Active Directory</b>	<a href="#">Información general de Servicios de certificados de Active Directory</a>
<b>Solución de problemas de seguridad</b>	<a href="#">Wiki: Portal de solución de problemas</a>

<b>Windows Server Update Services</b>	<a href="#">Introducción a Windows Server Update Services</a>
<b>Microsoft System Center</b>	<a href="#">Microsoft System Center 2012</a>

© 2016 Microsoft