Visor de Eventos

Transcribed on August 5, 2025 at 4:36 PM by Minutes AI

Speaker 1 (00:05)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema del visor de eventos.

Vamos a hablar de los registros en Windows Server, qué herramientas tenemos para poder monitorizar y ver esos registros, Hablaremos del visor de eventos, qué secciones tiene, hablaremos también de otros elementos como puede ser la suscripción de eventos o como podemos ver estos registros también desde Server Manager ya hablaremos de las directivas de grupo que nos van a permitir configurar estas características.

El registro de eventos nos provee información sobre el funcionamiento del sistema operativo, las aplicaciones y al clasificar los eventos en diferentes eventos de información o registros de información de advertencia, de error o de seguridad.

Y vamos a poder ver todos estos registros a través de una consola.

¿Que es el visor de eventos?

El visor de eventos podemos obtenerlo desde la parte de herramientas de Server Manager y nos va a permitir ver los registros que se van generando en el sistema operativo.

Es importante entender que los registros que se generan en el sistema operativo dependen de muchas cosas.

Va a haber una serie de registros que se generan de forma automática en sistema, las aplicaciones están preparadas para generar esos registros y luego hay otros registros que tenemos que configurar algo o que tenemos que habilitar algo previamente.

Ese tipo de registros, por ejemplo, cuando nosotros queremos hacer unas pruebas de debugging de una determinada aplicación o de un determinado servicio rol, a lo mejor tenemos que habilitar una serie de características para que se genere el software.

En lo que se refiere a la parte de seguridad también nos pasa lo mismo, hay ciertas auditorías que nosotros tenemos que activar para que se generen esos registros.

Si nosotros no hacemos esa configuración previa, pues no se van a activar esos registros, sino podremos verlos desde el visor de eventos o de otra herramienta que sea capaz de extraer esos registros de eventos.

El visor de eventos para facilitar el poder consultar la información, va a dividir la información en diferentes secciones que a su vez cada una de estas secciones va a tener una categoría o varias para clasificar la información.

Vamos a tener unas vistas personalizadas, si estamos en Windows Server además vamos a tener una serie de vistas específicas por cada uno de los roles y esto nos va a permitir ver los registros que tienen que ver con el servicio de DNS o los registros que tienen que ver con el directorio activo o con el servicio de DHCP o con el servicio web.

Dentro de estas vistas personalizadas nosotros podemos generar nuestra propia vista personalizada para tener una vista con los eventos que nosotros queremos monitorizar.

Luego dentro de los eventos de Windows se van a clasificar en eventos de aplicación, de seguridad, de inicio de sesión, de sistema y eventos reenviados.

Los eventos reenviados es cuando nosotros configuramos una suscripción para que otro dispositivo nos envíe los registros, pues vamos a ver esos registros en esa sección.

Luego tendríamos la parte de aplicación.

En la parte de aplicación nosotros vamos a ver los eventos organizados por aplicación, por fabricante.

Dentro de Microsoft vamos a tener Windows y dentro de Windows vamos a tener todos los componentes de Windows.

Con lo cual nosotros podemos ver, por ejemplo, los eventos que tienen que ver con bitlocker o los eventos que tienen que ver con un determinado componente de Windows, con un servicio como DFS o con la parte de cifrado.

Esto nos facilita mucho cuando nosotros estamos analizando por qué no funciona un determinado componente, ir a ver específicamente aquellos registros que pertenecen a ese componente.

Y luego tendríamos la parte de suscripción, que sería donde nosotros configuraríamos las suscripciones para enviar eventos o registros a otra máquina que actuaría como un servidor central, como un contenedor central para recibir esos registros.

Desde Server Manager nos vamos a la parte de Tools y tenemos aquí el visor de eventos.

Si nosotros habilitamos el visor de eventos nos va a cargar aquí los registros del dispositivo.

Y si nos vamos a la parte de vistas personalizadas vemos que lo primero que tenemos aquí son vistas relacionadas con los roles del servidor.

En este caso este servidor no tiene ningún rol instalado, con lo cual lo que tendríamos aquí serían los eventos administrativos y tendríamos aquí los servicios de escritorio remoto.

Si nosotros seleccionamos cualquier evento, por ejemplo la parte de eventos administrativos, seleccionamos podemos ver las propiedades de ese evento.

Aquí tendríamos la parte de detalles con información del evento y además, en algunos casos puede incluso indicarnos posibles soluciones, no sólo lo que está sucediendo, el tipo de error, sino que además posibles soluciones.

Luego podríamos buscar información online de ayuda relacionada con ese evento.

Y luego otra cosa que nosotros podemos hacer es que podemos anclar una tarea a un determinado evento.

Entonces cuando nosotros sabemos que se va a producir ese evento, podemos programar que se realice una determinada función.

Podemos seleccionar en este caso que se inicie un programa, que se envíe un correo o que se muestre un mensaje Esta es una opción muy interesante porque si yo por ejemplo conozco el evento en el que hay un fallo a la hora de iniciar sesión con un usuario, puedo hacer que me envíe un correo, entonces siempre que ese usuario, que el usuario administrador tiene un fallo a la hora de iniciar sesión, me va a enviar un correo.

Si uno de los empleados está tratando de iniciar sesión y se equivoca una o dos veces, voy a recibir dos correos, pero si de repente recibo 15 correos o 20 correos o 30 correos de que hay un falto inicio de sesión relacionado con el administrador del dominio, pues automáticamente puedo entender que se está tratando de realizar un ataque contra esa cuenta.

Entonces el visor de eventos me puede ayudar a detectar pues un ataque, en este caso sobre una determinada identidad o puedo hacer que se lance una tarea y que se lance un script para levantar un servicio cuando se cae un determinado rol o un determinado servidor.

De esta manera yo voy a poder solucionar un problema de forma automatizada.

También tenemos la posibilidad de grabar los eventos y de esta manera poder utilizar después esos eventos para enviárselos a alguien, para poder consultarlo con otro compañero, etc.

Tenemos aquí lo que sería la parte de filtros, donde podemos generar diferentes filtros o podemos importar filtros y una de las cosas que nosotros podemos hacer es que podemos crear nuestro propio filtro.

Yo puedo seleccionar un filtro que sea por ejemplo de los últimos 30 días, que sean de temas críticos, error y advertencia y que sea por ejemplo dentro de la parte de Windows, específicamente la parte de seguridad, le ponemos nombre, entonces yo voy a tener un filtro que se va a generar con aquellos eventos que tienen relación en este caso con la seguridad en los últimos 30 días y que además eventos que sean críticos, que sean de error o que sean Word.

Luego tendríamos aquí la parte de Windows y dentro de los registros de Windows los tendríamos divididos por aplicación, los tendríamos divididos por seguridad.

Luego en la parte de seguridad veis que tenemos muchos registros que tienen que ver con lo que sería la parte de los inicios de sesión de diferentes servicios o diferentes cuentas cuando se crea un proceso, Special Logo, Credencial Validation.

Entonces tenemos monitorizados algunos aspectos de lo que es la seguridad de Windows de forma automatizada sin que nosotros tengamos que configurar nada, pues algunos eventos ya están habilitados, ya están activados otros eventos.

Veremos en vídeos posteriores que tenemos que nosotros hacer una configuración previa para que se generen esos registros.

Tendríamos la parte de Inicio, la parte de Sistema y aquí si tuviéramos eventos que se enviaran desde otros dispositivos que los hubiéramos configurado aquí en la parte de suscripción, pues los veríamos en eventos reenviados.

Otro elemento interesante del visor de eventos es en la parte de aplicaciones.

Veis que tenemos Microsoft, tendríamos aquí Windows y luego dentro de Windows lo vamos a tener clasificado por componentes.

Esto es muy interesante porque nos va a permitir verificar los eventos que están relacionados con una determinada función o un determinado componente.

Por ejemplo, si yo estoy trabajando como App Locker para bloquear archivos, para bloquear ejecutables o para bloquear paquetes de instalación, pues puedo ver aquí los eventos relacionados con ese elemento.

Si yo, por ejemplo, estoy teniendo problemas de directivas de autenticación, pues puedo ver aquí los eventos relacionados con las directivas de autenticación, con la Protección del Cliente, con Métodos de autenticación, con el sistema de backup.

Muchos de estos eventos o muchas de estas categorías no van a tener registros porque nosotros no tenemos habilitado ese servicio porque yo no estoy utilizando el servicio de backup todavía en esta máquina, entonces no voy a tener registros.

Pero si yo tuviera problemas con el servicio de backup, podría venir específicamente a ver aquellos registros que tienen que ver con el servicio de backup.

Otro elemento que tenemos disponible que está relacionado con el visor de eventos es la suscripción de eventos.

La suscripción de eventos nos va a permitir recopilar eventos de otro dispositivo o enviar eventos a otro dispositivo mediante la suscripción de eventos.

De esta manera podemos generar incluso servidores que actúen como contenedores centrales para la suscripción de eventos de diferentes equipos.

Y esto tiene sus ventajas porque en un momento determinado una actividad maliciosa o un malware o un atacante puede tratar de borrar registros para ocultar su actividad.

Si esos registros se han enviado a otra máquina diferente, pues va a ser más difícil que pueda eliminar esos registros.

De esta manera, si nosotros estamos haciendo un análisis sobre una determinada máquina, vamos a tener registros más fiables que los que abría la propia máquina.

Otra situación puede ser que una máquina deje de funcionar y no podamos acceder a los registros de esa máquina.

Sin embargo, si esos registros se han enviado a una máquina diferente, podemos analizar esos registros y puede ser un indicativo que nos pueda ayudar a entender por qué esa máquina dejó de funcionar.

Para habilitar la suscripción de eventos tenemos que seguir los pasos que tenemos en la diapositiva.

El equipo que va a recopilar los datos tiene que ser administrador local de cada equipo que es origen de esos datos.

Tiene que tener permisos para poder recopilar esos datos.

En todos los equipos que sean origen de datos, es decir, los que van a enviar esos eventos, hay que ejecutar una consola con privilegios con el comando winrm quickconfig.

El equipo que va a actuar como almacén central para esos eventos tiene que ejecutar en una consola el comando webutilqc.

Luego tiene que configurar la suscripción y después podemos verificar la replicación en la sección de eventos reenviados.

En esa sección veremos los eventos y los vamos a ver con el nombre de una máquina que sea el nombre de la máquina que originó esos registros.

Podemos ver también los eventos desde Server Manager.

Nosotros en Server Manager tenemos una parte donde tenemos los registros de eventos y además podemos personalizarla.

Podemos abrir las características y seleccionar que eventos queremos que se vean en la parte de Server Manager.

Hay que tener en cuenta que si habilitamos muchos eventos para ver en Server Manager, vamos a hacer que la consola de Server Manager vaya más lenta, Entonces hay que tener precaución en la cantidad de eventos que vemos desde Server Manager.

Y luego también podemos configurar los registros mediante objetos de directiva de grupo.

Podemos tener una configuración centralizada que podríamos hacer en la dirección que tenéis en la diapositiva dentro de Configuración de equipo, Directivas, plantillas administrativas, componentes de Windows.

Y ahí tendríamos los servicios de registros de Windows.

Como conclusión hemos visto que tenemos una serie de registros que nos pueden dar mucha información de lo que estaba funcionando y lo que está sucediendo con el sistema operativo y las aplicaciones y que además podremos incluso almacenar estos registros de forma centralizada.

Tenemos una guía en la URL que tenéis en la diapositiva en la que tendríais información sobre todos los registros específicos de seguridad y auditoría de Windows 10 y Server 2016, aunque las últimas versiones estaríamos hablando de Windows 11 y Server 2022, pero muchos de los registros de seguridad y auditoría tienen los mismos códigos y son registros comunes.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.