Kaseya 2

Standard Solution Package

Guía del usuario

Versión R8

Español

October 23, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contenido

Capítulo 1

Introducción

En este capítulo

Introducción

El **Standard Solution Package** es un conjunto de objetos de datos, llamado de manera colectiva **contenido**, cargado previamente en el VSA. Kaseya definió este contenido para reflejar cuáles son las soluciones basadas en las mejores prácticas para administrar máquinas dentro de un entorno de cliente. El contenido, junto con la documentación y las metodologías, está diseñado para ayudar a los administradores de Kaseya a aplicar de forma rápida y coherente un conjunto estándar de soluciones de configuración recomendadas inmediatamente después de la implementación de los agentes.

Funciones y capacidades

Entre las funciones y capacidades se incluyen mejoras de usabilidad del producto, auditoría e inventario, soporte remoto, administración de parches, supervisión y alertas, directivas, automatización, elaboración de informes, etc.

Módulos admitidos

En este paquete encontrará contenido y soporte relacionados con los módulos y las funciones principales de Kaseya K2 (versión 6.3) tales como sistema, agente, auditoría, control remoto (incluido LiveConnect), administración de parches, supervisión, procedimientos de agente, Info Center, vistas y administración de directivas.

Software y plataformas de SO admitidos

Plataformas de SO de agentes admitidas

Este paquete proporciona contenido y soporte relacionados con las siguientes plataformas de SO en las máquinas de los agentes.

- Microsoft Windows XP, 2003, 2003 R2, Vista, 2008, 2008 R2, 7, 2012
- Apple Macintosh Mac OS X 10.5 (Leopard), 10.6 (Snow Leopard), 10.7 (Lion), 10.8 (Mountain Lion)
- SuSE Linux Enterprise 10 y 11, Red Hat Enterprise Linux 5 y 6, Ubuntu 8.04 y superiores, y OpenSuSE 11, CentOS 5 y 6

Sistemas de terceros admitidos

En ITSM-SS, encontrará contenido y soporte relacionados con los siguientes sistemas y aplicaciones de terceros.

- Correo electrónico y mensajería
  - Exchange 2003, 2007, 2010, SMTP, IMAP, POP3, servidor Blackberry Enterprise Server
- Antivirus y antimalware
  - Symantec AntiVirus v10, Corporate Edition v10, Endpoint Protection v11
  - McAfee VirusScan/Enterprise, Total Protection, Endpoint Protection
  - Sophos AntiVirus
  - Trend Micro OfficeScan v10, Worry-Free Business Security v11
  - Antivirus AVG Technologies v8
  - Kaspersky Endpoint Security v8
  - Microsoft Security Essentials, Forefront Endpoint Protection
  - Productos antivirus y antimalware de terceros integrados en el Centro de seguridad de Microsoft
- Copias de seguridad y recuperación

  - Symantec Backup Exec v10/11/12/12.5/2010/2012
  - Computer Associates BrightStor ARCServe Backup r11.1/11.5/12/12.5/15
- Servidores de bases de datos
  - Microsoft SQL Server 2005/2008/2008 R2
- Acceso remoto
  - Terminal Server, Citrix MetaFrame/Presentation Server/XenApp
- Infraestructura de red
  - Active Directory de Microsoft, Archivos e impresión, servidor DHCP, servidor DNS, servidor FTP
- Servidores web
  - Microsoft IIS 6/7, SharePoint Server 2007/2010

Resumen del paquete

El **Standard Solution Package** de contenido se carga previamente de manera automática en el VSA. Algunos tipos de contenido se organizan mediante el **gabinete Sistema** en un árbol de objetos de datos. Este contenido incluye lo siguiente:

- **Directivas**: Administración de directivas > Directivas
- **Procedimientos de agente**: Procedimientos de agente > Crear/Programar
- **Conjuntos de monitores**: Supervisar > Conjuntos de monitores

Otros tipos de contenido se muestran en listas desplegables exclusivas:

- **Vistas**: al seleccionar la lista desplegable **Vista** en la parte superior de cualquier página de máquina donde se muestra el filtro ID de máquina/ID de grupo, se muestra una lista de *vistas* predefinidas con el prefijo `zz[SYS]`.
- **Directivas de administración de parches**: al seleccionar la lista desplegable **Directiva** en **Administración de parches > Aprobación por directiva**, se muestra una lista predefinida de *directivas de aprobación y denegación de administración de parches* con el prefijo `zz[SYS]`.
- **Conjuntos de eventos**: al seleccionar la lista desplegable **Definir eventos para correspondencia u omisión** en **Supervisar > Alertas de registro de eventos**, se muestra una lista predefinida de *conjuntos de eventos* con el prefijo `zz[SYS]`.

Foco de los servicios de TI

El **Standard Solution Package** está orientado a la prestación de servicios más frecuentes de TI que suelen brindar los proveedores de servicios de TI o las organizaciones de soporte de TI. Entre estos servicios se incluye lo siguiente:

Servicio de TI	Descripción
Configuración predeterminada	Permite una administración simplificada de la configuración y el aprovisionamiento de los ajustes básicos y las directivas de notificación de soporte remoto.
Auditoría/Inventario	Proporciona datos de inventario de hardware y software actualizados para las máquinas.
Administración de parches/actualizaciones	Proporciona capacidades de administración de parches y actualizaciones para mejorar la estabilidad y reducir las vulnerabilidades y los riesgos asociados a estas, y visibilidad del estado de los parches de las máquinas.
Mantenimiento de rutina	Realiza el mantenimiento de rutina a las máquinas para mantenerlas en funcionamiento de manera más eficaz.
Monitoreo	Lleva a cabo una supervisión continua de los servidores o las estaciones de trabajo para garantizar la disponibilidad de servicios, datos de rendimiento, procesos, eventos, estado y disponibilidad en general.

Generación de Reportes	Proporciona capacidades de elaboración de informes que permiten visualizar todos los aspectos de los distintos servicios de soporte de TI que se prestan.

Configuración automatizada y específica del sistema

Hay contenido que se aplica, en general, a todas las máquinas administradas. El resto del contenido predefinido representa un catálogo de soluciones alternativas conocidas cuya aplicación se puede considerar bajo circunstancias específicas.

- **Configuración automatizada del sistema**: el contenido que se usa con mayor frecuencia se puede configurar de forma rápida y automática para una organización en particular por medio del asistente para configuración **Systems Management Configuration**. Simplemente siga los pasos que se detallan en la sección **Configuración de administración de sistemas** *(página 6)* de esta guía. El contenido que usa el asistente se describe en la sección **Contenido habilitado del asistente para configuración** *(página 19)* de esta guía.
- **Configuración específica del sistema**: una vez que ejecuta el asistente para configuración **Systems Management Configuration**, puede modificar las directivas aplicadas. También puede seleccionar contenido y directivas adicionales o diferentes y reorganizar la configuración inicial para adaptarla a las necesidades de su empresa. Esta capacidad de personalización se presenta en el tema **Personalización de las directivas de una organización** *(página 14)*. En la sección **Catálogo de contenido completo** *(página 67)* de esta guía, se describen los objetos de datos que están a su disposición.

Capítulo 2

Configuración de administración de sistemas

En este capítulo

Asistente para configuración

La versión 6.3 del **Virtual System Administrator™** de Kaseya incorpora el asistente para configuración **Systems Management Configuration**. El asistente de configuración le permite *configurar y aplicar las políticas de administración de la máquina rápidamente para una organización específica.* Una vez configuradas, estas políticas se asignan a cada máquina que administra en nombre de esa organización. Las políticas rigen varios aspectos diferentes de la administración de la máquina:

- Programación de auditoría
- Monitoreo
- Alertas
- Administración de Parche
- Mantenimiento de rutina de la máquina utilizando procedimientos de agente

Con las políticas, ya no tiene que administrar cada máquina en forma individual. Sólo tiene que asignar o cambiar la política. La asignación o el cambio de una política dentro de una política asignada se propaga en los 30 segundos posteriores a las máquinas de todos los miembros sin la necesidad de realizar una programación. Una vez aplicadas, puede determinar rápidamente si las máquinas administradas cumplen o no con sus políticas asignadas. El rastreo del cumplimiento a partir de políticas individuales le brinda la información necesaria para distribuir los servicios de TI sistemáticamente a través de las organizaciones que administra.

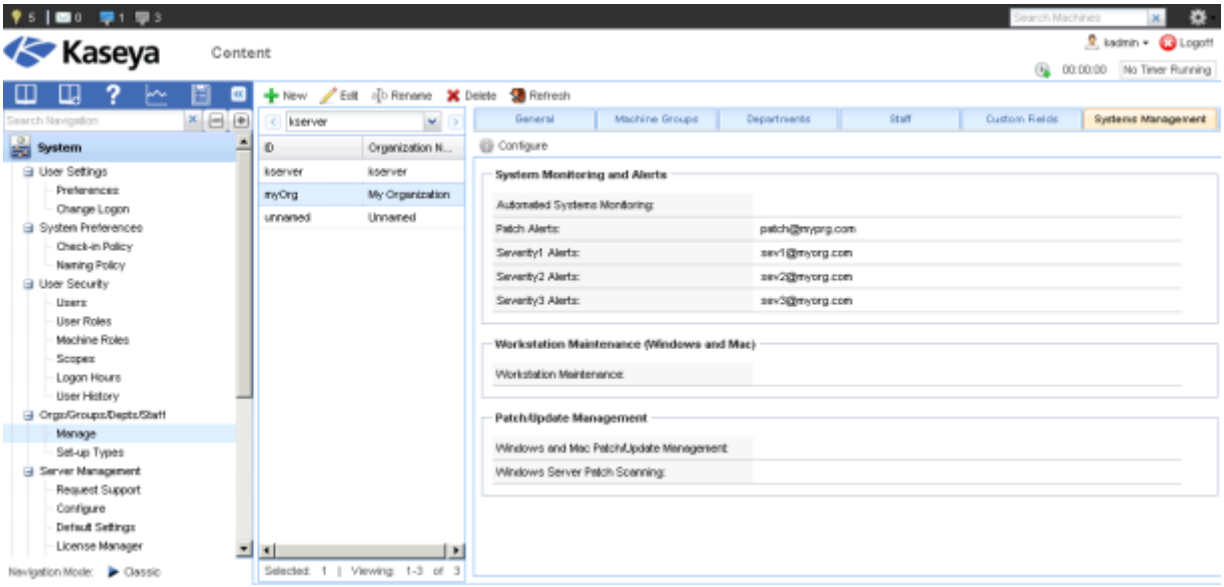
Antes de ejecutar el asistente para configuración **Systems Management Configuration** en cualquier organización, tenga en cuenta los siguientes puntos.

- Puede volver a ejecutar el asistente para configuración **Systems Management Configuration**, a fin de seleccionar diferentes opciones para la organización, siempre que no haya personalizado las asignaciones de directivas para la misma organización en **Policy Management**.
- Si ejecuta el asistente para configuración **Systems Management Configuration**, significa que tiene la intención de administrar dicha organización *según las directivas*. Al modificar la configuración del agente *de forma manual* después de aplicar una directiva, se genera una condición de “sustitución de directiva”. Por ejemplo, la implementación de cambios en el menú de agente de una máquina en la página **Menú de agente** en el módulo **Agente** establece una condición de sustitución para esa máquina con agente. Las directivas sustituidas de **Policy Management** serán omitidas a partir de ese momento. Siempre es posible borrar una directiva sustituida por medio del módulo **Policy Management**.

Ejecución del asistente para configuración

1. Navegue a la página **Administrar** en **Sistema > Orgs/Grupos/Deptos/Personal**.
2. Seleccione una organización en el panel central.
3. Seleccione la pestaña **Administración de sistemas**.
4. Haga clic en el botón **Configurar**.

Nota: En un nuevo VSA sin agentes instalados, es posible que la barra de notificación le indique ejecutar este mismo asistente para configuración para la organización `myOrg`.



En esta sección

Página 1 del asistente para configuración - Supervisión y alertas del sistema

- **Habilitar supervisión automatizada de sistemas**: cuando el sistema encuentra un elemento para alertar, genera una alarma y le notifica por correo electrónico.
- **Alertas de parches**: la dirección de correo electrónico exclusiva para recibir notificaciones de alertas de parches.

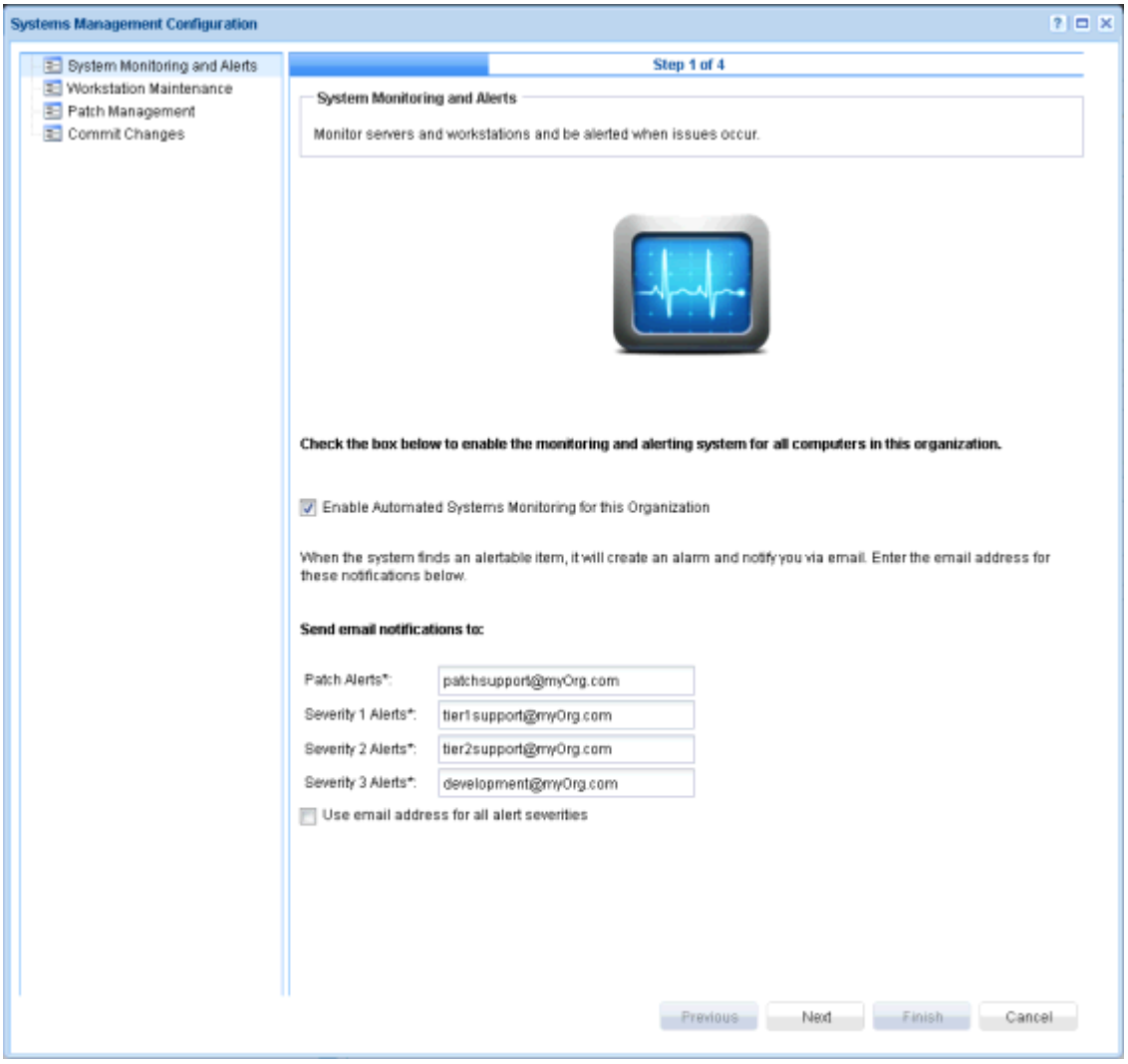
  Nota: Esta dirección de correo electrónico no se usa, a menos que se activen las casillas de verificación de la **página del asistente para administración de parches** *(página 9)*.

- **Usar la dirección de correo electrónico para todas las alertas**: desactive esta casilla de verificación para visualizar tres campos adicionales de *alertas de gravedad*. Active esta casilla de verificación para usar la misma dirección de correo electrónico en el cuadro de edición **Alertas de parches** para los cuatro tipos de alertas.

  Se entiende por “alertas de gravedad” todas aquellas *que no son Alertas de parches.* Algunos tipos de alertas se consideran más graves que otros. Una organización de TI puede tener varios equipos, y cada uno de estos puede responder a diferentes niveles de alertas.

  - **Alertas de gravedad 1**: la dirección de correo electrónico para alertas de nivel bajo.
  - **Alertas de gravedad 2**: la dirección de correo electrónico para alertas de nivel medio.
  - **Alertas de gravedad 3**: la dirección de correo electrónico para alertas de nivel alto.

Nota: A fin de habilitar el uso de las mismas directivas integradas estándar por parte de varias organizaciones en **Policy Management**, se introducen marcadores de posición que representan **tokens** en los campos de directivas que requieren una dirección de correo electrónico. Estos valores de token son `#patchAlertEmail#`, `#sev1AlertEmail#`, `#sev2AlertEmail#` y `#sev3AlertEmail#`. El VSA reemplaza de forma automática un valor de token en una directiva por la dirección de correo electrónico apropiada para una organización en particular cuando se envía una notificación de alerta. Las direcciones de correo electrónico de la organización a las que hacen referencia los tokens se especifican por medio de esta página del asistente. Las categorías de directivas de **Policy Management** que incluyen direcciones de correo electrónico son **Alertas**, **Conjuntos de monitores** y **Configuración de parches**.

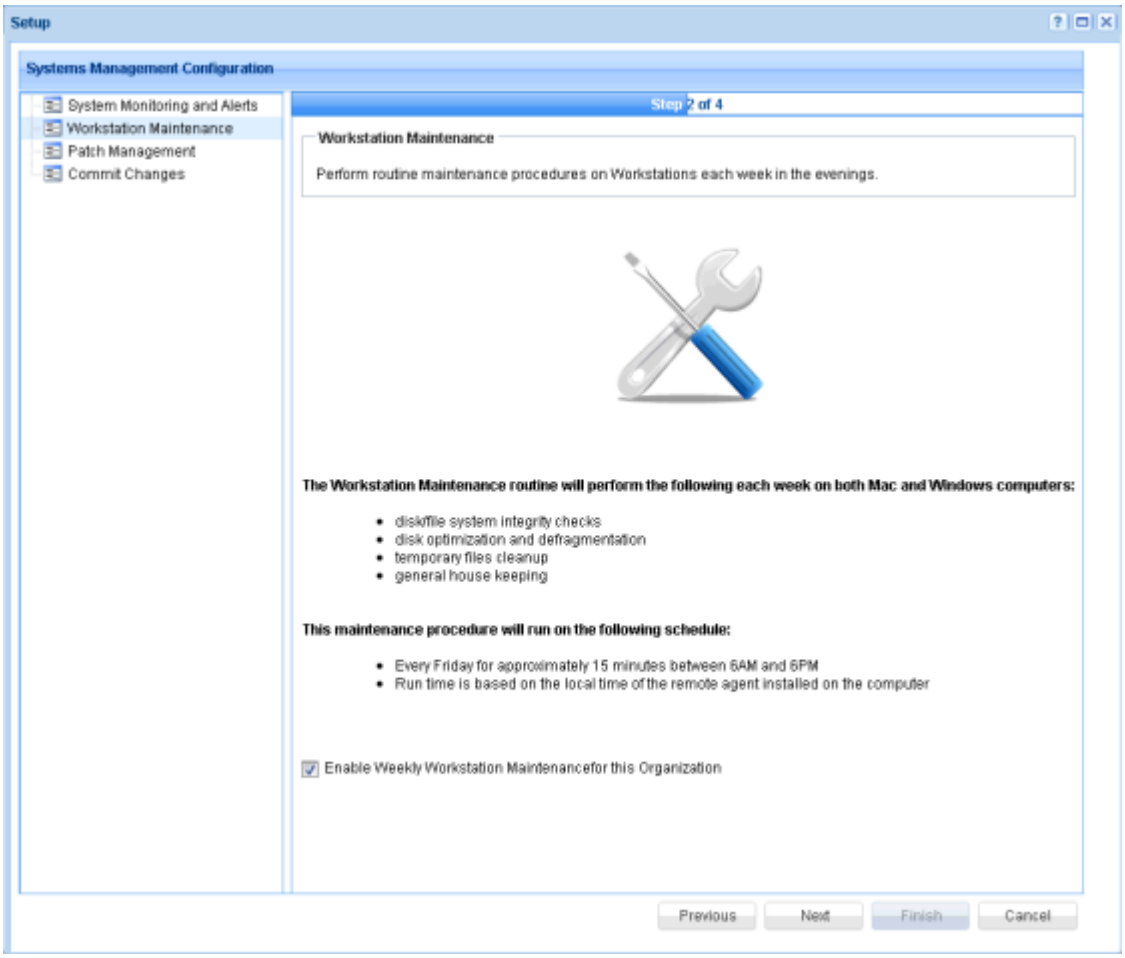


Página 2 del asistente para configuración - Mantenimiento de la estación de trabajo

- **Habilitar mantenimiento semanal de la estación de trabajo**: si está seleccionada, se ejecutan rutinas de mantenimiento de la estación de trabajo una vez por semana, de lunes a viernes, entre las 18:00

y las 06:00 h. Sólo se aplica a estaciones de trabajo Windows y Macintosh. No se aplica a Linux. Esto incluye:

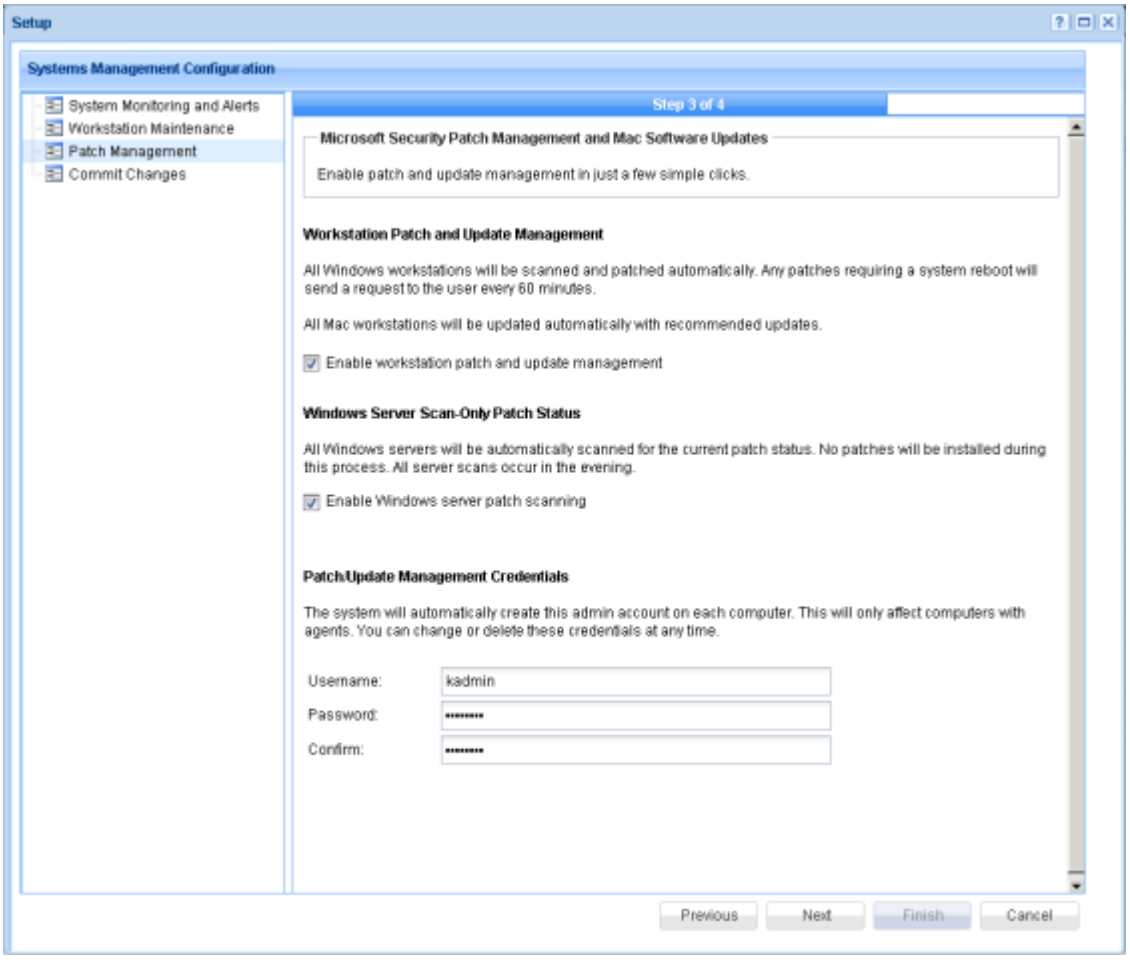
- Comprobaciones de integridad del sistema de discos y archivos
- Optimización y desfragmentación del disco
- Limpieza de archivos temporales



Página 3 del asistente para configuración - Administración de parches

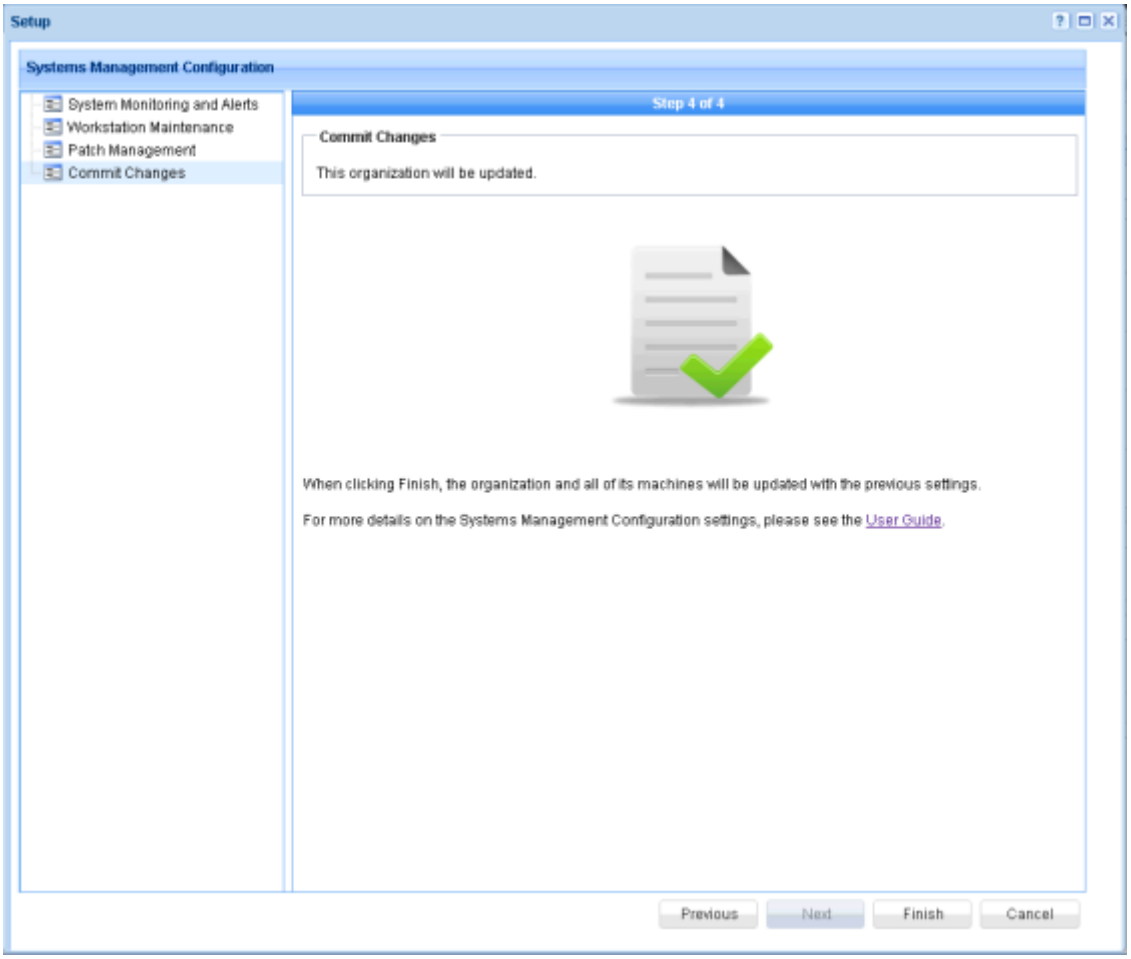
- **Habilitar administración de parches y actualizaciones de la estación de trabajo**: si está seleccionada, se examinarán e instalarán parches automáticamente en todas las estaciones de trabajo Windows. Si un parche requiere un reinicio, el usuario recibe una solicitud cada 60 minutos para que permita que se lleve a cabo el reinicio.
- **Habilitar detección de parches de servidores Windows**: todos los servidores Windows se analizan automáticamente para detectar su estado actual. No se instalarán parches durante el proceso. Todos los exámenes de servidores se realizarán por la noche. La aplicación de parches para servidores debe realizarse de manera manual.
- **Credenciales para administración de parches**: el sistema crea esta cuenta de administrador automáticamente en cada computadora. Eso solo afectará a las computadoras con agentes. Puede cambiar o eliminar estas credenciales en cualquier momento.

Nota: Se agrega una credencial para esta cuenta nueva en la página Administrar credenciales en Auditoría para esta organización. La credencial nueva se designa como credencial de agente, lo que significa que se configura para funcionar como la credencial del agente cuando se ejecuta una directiva habilitada por **Systems Management Configuration** para esta organización.



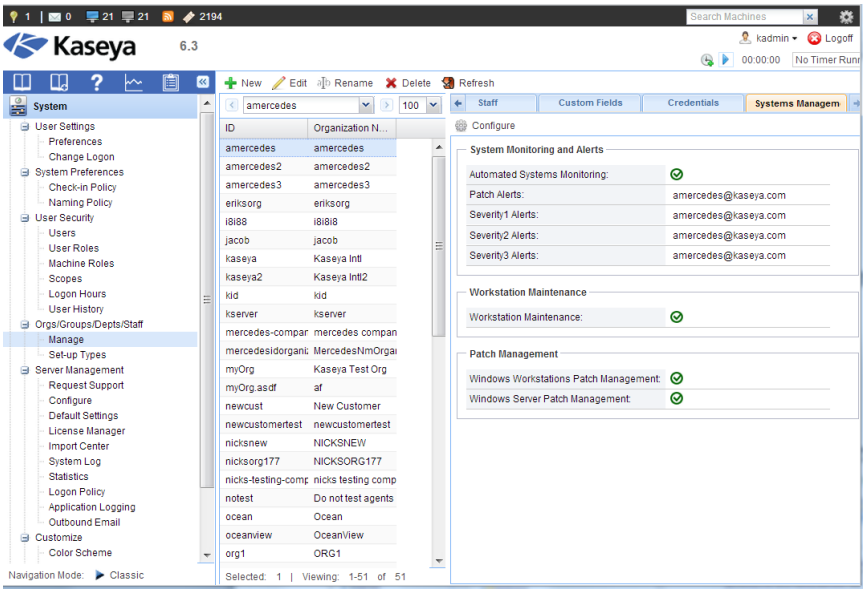
Página 4 del asistente para configuración - Configuración finalizada

Después de hacer clic en el botón **Finalizar**, un cuadro de mensaje confirma que la solicitud está siendo procesada y que llevará unos 5 minutos. Las directivas para esta organización se crearán y aplicarán a sistemas con agentes que pertenezcan a ella.



Confirmación en la pestaña Administración del sistema

Cuando se cierra el asistente para configuración **Systems Management Configuration**, es posible que la aplicación de las directivas a las máquinas administradas en la organización seleccionada demore hasta 5 minutos. Luego verá casillas de verificación de color verde en la pestaña **Administración del sistema** que confirmarán la aplicación de las opciones que seleccionó. Las directivas aplicadas pueden tardar 30 minutos o más en propagarse a las máquinas administradas en esa organización.



Distribuir Agentes

En este momento, la única tarea pendiente consiste en agregar las máquinas administradas a una organización. Existen varias maneras de implementar agentes.

- **Discovery**: si ya tiene al menos un agente instalado en una red, el método recomendado para detectar e instalar agentes consiste en usar el **móduloDiscovery** *(http://help.kaseya.com/webhelp/ES/KDIS/R8/index.asp#7293.htm)*. Al detectar una red nueva, es posible que la barra de notificación le solicite ejecutar la detección de redes.
- **Implementación de agentes**: si está implementando el *primer* agente en una red nueva, vaya a la página **Implementar agentes** *(http://help.kaseya.com/webhelp/ES/VSA/R8/index.asp#491.htm)* página en Agente. Consulte la guía de inicio rápido de **Implementación de agentes** *(http://help.kaseya.com/webhelp/ES/VSA/R8/ES_agentdeployment_R8.pdf#zoom=70&navpanes=0)* para obtener una introducción de la instalación de agentes.

Recuerde que el asistente para configuración **Systems Management Configuration** sólo aplica directivas a la organización que se acaba de seleccionar. Asegúrese de que los agentes que implemente se asignen a la misma organización.

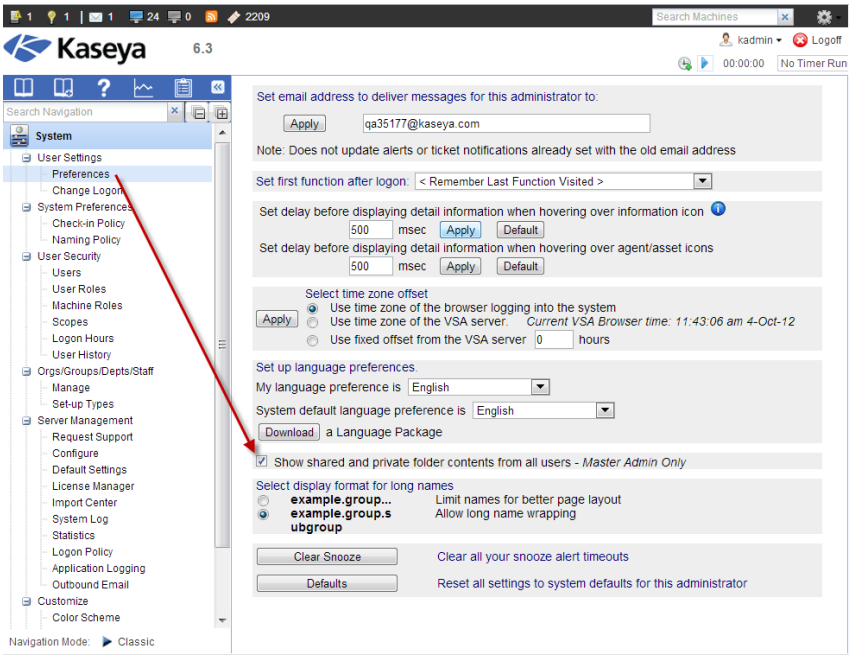
¿Cómo funciona?

En la sección **Asistente para configuración** *(página 6)*, sólo se abordó el modo en que se usa el asistente para configuración **Systems Management Configuration**. Si eso es todo lo que necesita saber, puede omitir esta sección. Ahora bien, si le interesa saber de qué manera **Systems Management Configuration** saca provecho de la funcionalidad del VSA, continúe leyendo.

En esta sección

Requisitos previos

1. Asegúrese de haber iniciado sesión en el VSA como un *administrador maestro* en un VSA local o como un *administrador del sistema* en un VSA basado en la nube. De este modo, se asegura el acceso a las funciones que se abordan en esta sección.
2. Asegúrese de que la casilla de verificación **Mostrar contenido de carpetas compartidas y privadas de todos los usuarios - Sólo administrador maestro** esté activada en **Sistema > Configuración del usuario > Preferencias**. Esta casilla de verificación adicional permite ver las carpetas del gabinete Sistema que se describen en esta sección.

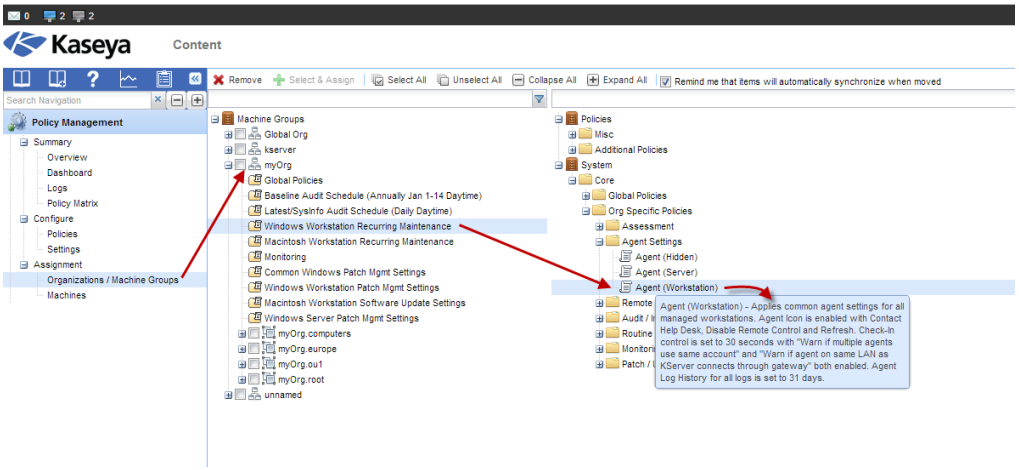


Directivas del sistema en Administración de directivas

Las opciones seleccionadas en el asistente para configuración **Systems Management Configuration** crean una lista de directivas que se aplican a la organización que se eligió. Siga los

pasos que se describen a continuación para ver esas directivas.

1. Navegue al módulo **Policy Management**.
2. Seleccione la página **Organizaciones/Grupo de máquinas**.
3. Para la misma organización que seleccionó al ejecutar el asistente para configuración **Systems Management Configuration**, expanda la carpeta en el panel central.
4. Expanda el gabinete **Sistema** en el panel de la derecha.



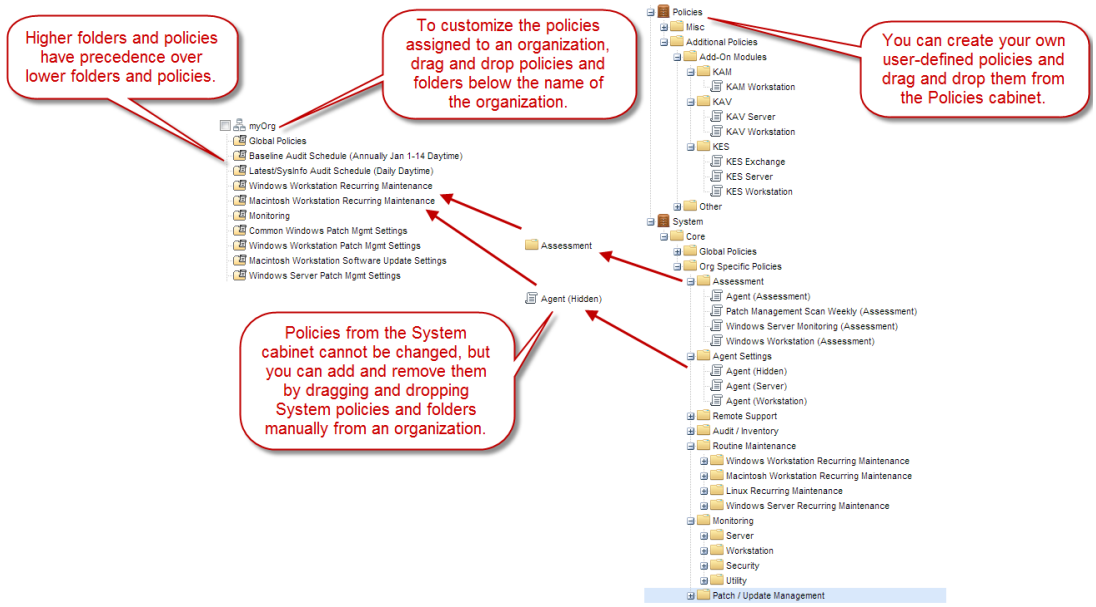
Observe que todas las carpetas asignadas a su organización tienen una carpeta correspondiente en el panel de la derecha. Esa carpeta suele contener subcarpetas que, a su vez, contienen conjuntos de directivas. Mantenga el mouse sobre cualquier directiva específica para ver la descripción de esta directiva predefinida. Cada máquina administrada en la organización seleccionada ahora se administra bajo esta directiva y todas las demás directivas asignadas a esta organización.

Personalización de las directivas de una organización

Incluso sin tener conocimiento acerca de cómo se configuran las directivas en detalle, puede comenzar a personalizar las directivas que se asignan a una organización específica.

En la página **Organizaciones/Grupo de máquinas** en Policy Management, puede personalizar las directivas asignadas a una organización arrastrando y soltando en forma manual carpetas o directivas desde el árbol de organización y hacia él. Esto implica eliminar de una organización directivas del gabinete Sistema, si así lo desea. Advierta que las **reglas de asignación de directivas** *(http://help.kaseya.com/webhelp/ES/KPM/R8/index.asp#8140.htm)* se aplican a la secuenciación de directivas que se incluyen debajo de una organización.

Se pueden arrastrar y soltar directivas y carpetas adicionales tanto desde el gabinete Sistema como desde el gabinete Directivas. Las directivas del gabinete Sistema no se pueden modificar, pero hay más directivas disponibles de este tipo que aquellas que se pueden seleccionar con el asistente para configuración **Systems Management Configuration**. Antes de intentar crear sus propias directivas definidas por el usuario, asegúrese de revisar las directivas del gabinete Sistema que se encuentran disponibles. En la sección **Contenido habilitado del asistente para configuración** *(página 19)* de este documento, se describe el conjunto completo de directivas del gabinete Sistema. Si desea saber más acerca de cómo se construye una directiva, consulte el tema **Detalles sobre directivas** *(página 15)*.

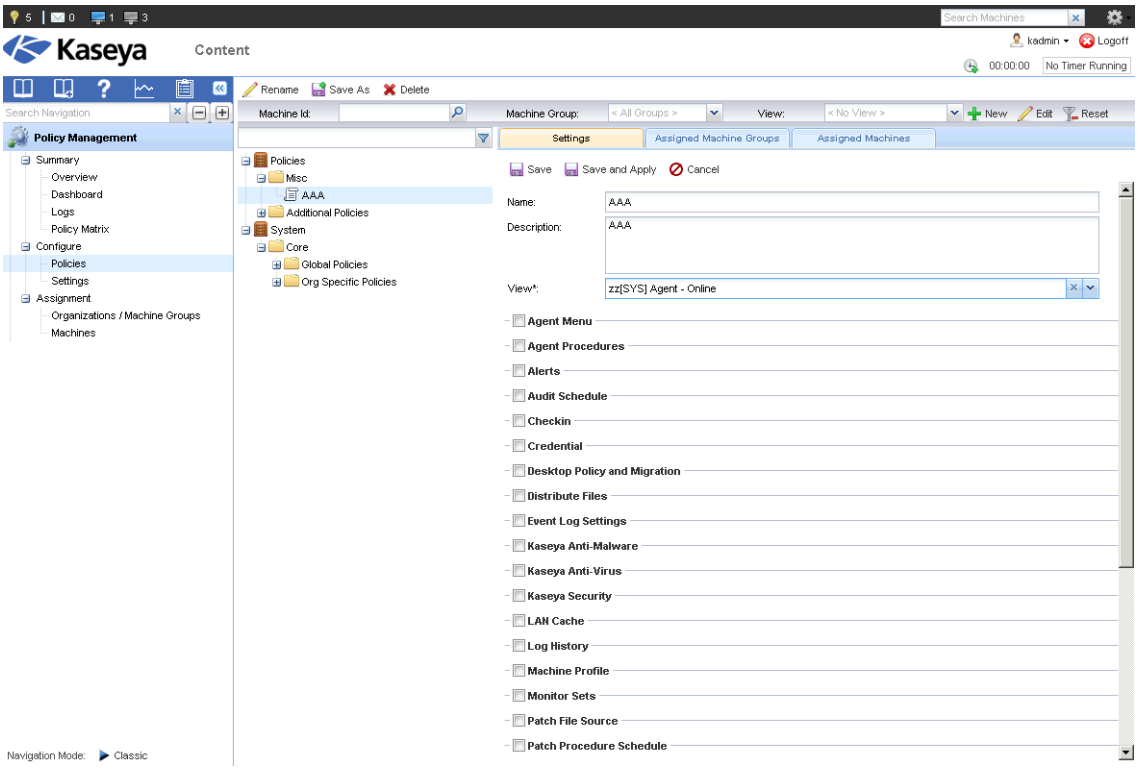


Detalles sobre directivas

Nota: Los siguientes tres temas describen de manera resumida el modo en el cual se construye una directiva. Para obtener más información acerca de las directivas, consulte la **guía del usuario y ayuda en línea sobre** *(http://help.kaseya.com/webhelp/ES/KPM/R8/index.asp#8410.htm)* **Policy Management**.

Los detalles de cada directiva, ya sea una de Sistema o una definida por el usuario, pueden revisarse en la página **Directivas**. Una directiva nueva puede incluir de forma opcional varias categorías diferentes de ajustes. Por ejemplo, una única directiva puede establecer propiedades de registro de agentes junto con una programación de auditoría y ejecutar procedimientos de agente al mismo tiempo.

La imagen siguiente muestra una lista parcial de las categorías de ajustes disponibles para usar cuando se crea una directiva nueva.

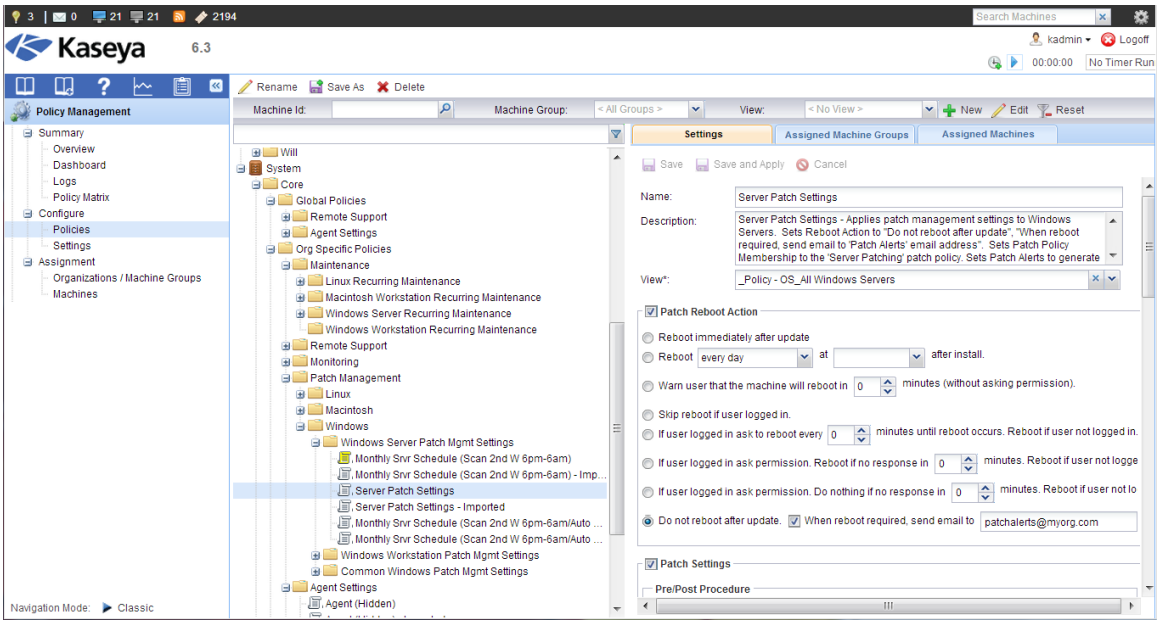


Configuración integrada y configuración específica de datos

Al revisar o configurar los ajustes de una directiva en particular, advertirá que existen dos tipos de ajustes:

- **Configuración integrada**: se suele establecer mediante casillas de verificación o botones de opción. Asigna la configuración a una máquina administrada, y eso es todo lo que se debe especificar en la directiva.
- **Configuración específica de datos**: especifica un *objeto de datos que existe en otro lugar del VSA.* Dicho objeto de datos puede formar parte del contenido estándar cargado previamente en el VSA, o bien, puede ser un objeto de datos que fue creado por otro usuario del VSA y que está siendo utilizado por este.

Por ejemplo, en la imagen siguiente, una directiva de Sistema predefinida muestra la directiva de "reinicio" de una máquina después de la actualización de los parches. Esta es una *configuración integrada* que no requiere especificación de ningún objeto de datos de su parte. En el siguiente tema, se aborda la *configuración específica de datos*.



Vinculación de directivas a objetos de datos

Establecer una configuración específica de datos en una directiva requiere especificar un objeto de datos en otra parte del VSA.

Recuerde que las directivas del gabinete Sistema en **Policy Management** son sólo un tipo de *contenido estándar* que se carga previamente al VSA. Entre otros tipos de contenido, se incluyen los siguientes:

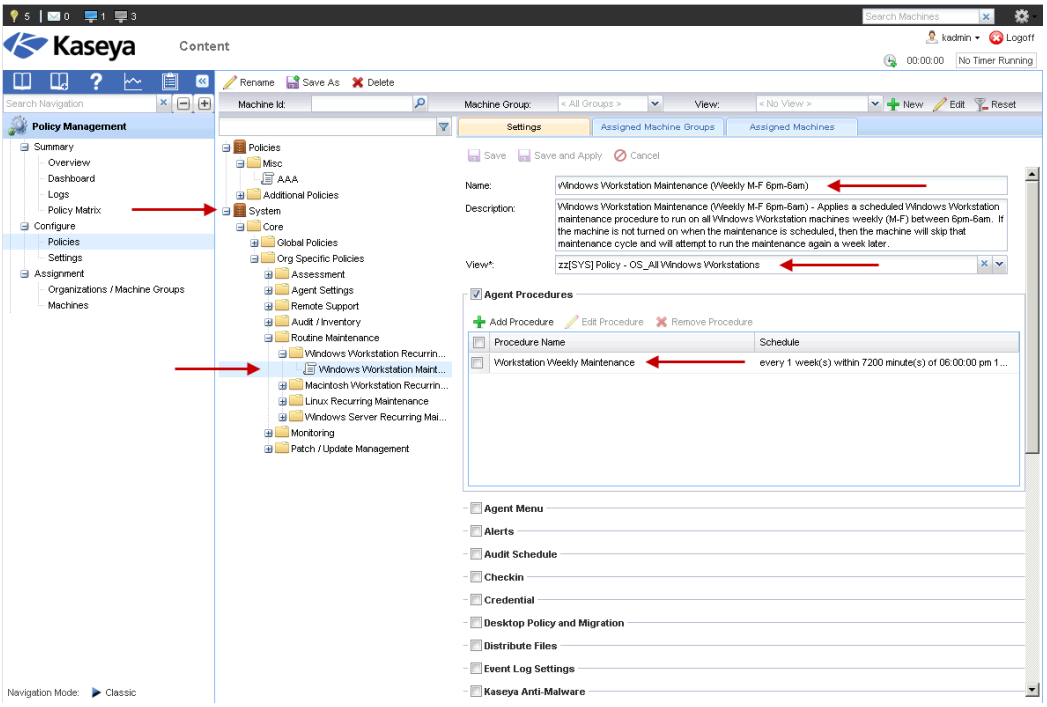
- Vistas
- Directivas de parches
- Conjuntos de Eventos
- Conjuntos de Monitores
- Procedimientos del Agente

Gran parte de las soluciones automatizadas que proporciona el asistente para configuración **Systems Management Configuration** se habilita por medio de la vinculación de las directivas predefinidas del gabinete Sistema con estos otros tipos de objetos de datos de Sistema predefinidos.

Por ejemplo, en la siguiente imagen, es posible visualizar los detalles de una directiva del gabinete Sistema llamada **Windows Workstation Maintenance (Weekly M-F 6pm-6am)**.

- Esta directiva programa la ejecución semanal del procedimiento de agente denominado **Workstation Weekly Maintenance**.

- Asimismo, advierta que esta misma directiva se encuentra restringida para las máquinas que pertenecen a la vista **zz[SYS] Policy - OS_All Windows Workstations**.



Esto es sólo un ejemplo del modo en que las directivas de Sistema están vinculadas al contenido de Sistema en otros lugares del VSA. Use este mismo método para revisar la configuración y los vínculos de cualquier otra directiva. Salvo por el hecho de que no es posible modificar las directivas y el contenido de Sistema, tenga en cuenta que no hay nada especial en su modo de configuración. Cuando se sienta listo para intentarlo usted mismo, cree sus propias directivas definidas por el usuario y su propio contenido para luego vincularlos entre sí, tal como se explica aquí. Si así lo desea, puede realizar una copia de una directiva de Sistema con el botón **Guardar como** y comenzar la personalización desde ese punto.

Nota: Para obtener más información acerca de las directivas, consulte la **guía del usuario y ayuda en línea sobre** *(http://help.kaseya.com/webhelp/ES/KPM/R8/index.asp#8410.htm)* **Policy Management**.

Capítulo 3

Contenido habilitado del asistente para configuración

En los siguientes temas, se resumen las capacidades del contenido que se desarrolló para ser utilizado con el asistente para configuración **Systems Management Configuration**. El mismo contenido se puede usar manualmente sin el asistente.

En este capítulo

Configuración predeterminada

Objetivo

Permitir una administración simplificada de la configuración y el aprovisionamiento de los ajustes básicos y las directivas de notificación de soporte remoto.

Introducción

Los agentes de Kaseya cuentan con un conjunto de ajustes de configuración que deben administrarse coherentemente en todas las máquinas administradas, por ejemplo: Menú de agente, Control de registro, Directorio de trabajo, Configurar credencial, Historial de registros, Configuración del registro de eventos y Directivas de notificación de control remoto. La Configuración de agente predeterminada aborda la necesidad de una administración coherente en todos los sistemas en lo que respecta a estos ajustes de configuración básicos de todo el sistema.

Políticas

Se proporciona un conjunto de directivas que aplican ajustes de configuración de agente predeterminados a todas las máquinas de la infraestructura de TI a la que se le brinda soporte. Estas directivas controlan ajustes tales como Menú de agente, Control de registro, Directorio de trabajo, Configurar credencial, Historial de registros, Configuración del registro de eventos y Directivas de notificación de control remoto, de acuerdo con un caso de uso sobre las mejores prácticas de operaciones generales en la configuración del sistema. Las directivas se encuentran en **[System].Core.Global Policies**, y se describen a continuación.

- **Configuración del Agente**
  - **Agent (Core)**: aplica la configuración de agentes común a todas las máquinas administradas. Se habilita el ícono de Agente, pero sólo la opción Actualizar está disponible. El Control de registro se establece en 30 segundos con las siguientes opciones habilitadas: “Advertir si varios agentes usan la misma cuenta” y “Advertir si un agente en la misma LAN que el KServer se conecta a través de la puerta de enlace”. El Historial de registros de los agentes para todos los registros se establece en 31 días.
  - **Windows Agent**: aplica la configuración de agente específica de Windows. Establece el Directorio de trabajo de agente en c:\kworking.
  - **Linux Agent**: aplica la configuración de agente específica de Linux. Establece el Directorio de trabajo de agente en /tmp/kworking.
  - **Macintosh Agent**: aplica la configuración de agente específica de estaciones de trabajo Macintosh. Establece el Directorio de trabajo de agente en /Library/kworking.
- **Remote Support**
  - **Server RC Notification Policy (Silent w Admin Note)**: aplica la configuración de notificación de control remoto en todos los servidores. Establece la opción Tomar control silenciosamente como tipo de notificación de usuario y habilita la opción Requerir nota del administrador para iniciar el control remoto.
  - **Workstation RC Notification Policy (Alert/Term w Admin Note)**: aplica ajustes de notificación de control remoto a todas las estaciones de trabajo. Establece las opciones “Si el usuario inició sesión, mostrar alerta” y “Notificar al usuario cuando finaliza la sesión” como tipo de notificación de usuario, y habilita la opción Requerir nota del administrador para iniciar el control remoto.

Auditoría/Inventario

Objetivo

Proporcionar una estrategia para realizar auditorías e inventarios de rutina, a fin de poder brindar soporte para la visibilidad de los activos de hardware y software para planeaciones a largo plazo, cumplimiento, proyectos a corto y largo plazo, respaldo para la toma de decisiones y solución de problemas.

Introducción

Kaseya admite varios tipos de auditorías basadas en agentes para detectar tanto hardware como software implementado en una infraestructura de TI. Entre estos se encuentran los siguientes tipos: última auditoría, auditoría de base y auditoría de información del sistema. Las últimas auditorías actualizan de manera gradual la información actual de las máquinas con respecto al hardware y al software. Las auditorías de base proporcionan la información de las máquinas con respecto al hardware y al software en un determinado momento. Las auditorías de información del sistema proporcionan detalles adicionales sobre el hardware por medio de SMBIOS. A fin de contar con información actualizada disponible acerca de las máquinas, y así poder tomar decisiones tácticas y estratégicas, es importante programar estas auditorías para que se ejecuten de acuerdo con un patrón regular periódico. Junto con esta información de auditoría, deben existir modos simples de ubicar tipos específicos de sistemas basados en los datos de inventario detallados que se conozcan sobre ellos, así como modos de elaborar informes sobre estos grupos de máquinas, en caso de que sea necesario, y actuar de manera efectiva con respecto a ellos.

Políticas

Se proporciona un conjunto de directivas que requieren la programación periódica de auditorías en todas las máquinas de la infraestructura de TI a las que se les brinda soporte. Estas directivas permiten la recolección de información fundamental para el caso de uso de servicio de Auditoría/Inventario. Las directivas se encuentran en **[System].Core.Org Specific Policies.Audit / Inventory**, y se describen a continuación.

- **Baseline.Baseline Audit Schedule (Annually Jan 1-14 Daytime)**
  - **Baseline Audit Schedule (Annually Jan 1-14 6am-6pm/Power Mgmt)**: aplica una auditoría de base anual programada para todas las máquinas implementadas y registradas. Comienza el 1 de enero y se extiende hasta el 14 de enero entre las 06:00 y las 18:00. La directiva usa la característica de administración de energía en el momento programado de la auditoría e intenta encender aquellas máquinas que estén apagadas antes de la auditoría. Esta directiva suele aplicarse en situaciones en las que se requieren auditorías anuales con fines de planeación o cumplimiento. También se usan para realizar comparaciones pertinentes entre auditorías de base y las últimas auditorías, a fin de llevar a cabo tareas operativas. La directiva puede aplicarse de forma selectiva a diversas máquinas, grupos de máquinas u organizaciones enteras de máquinas.
- **Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Daytime)**
  - **Latest/SysInfo Audit Schedule (Daily M-F 6am-6pm/Power Mgmt)**: aplica últimas auditorías y auditorías de información del sistema programadas a todas las máquinas registradas para que se lleven a cabo diariamente (de lunes a viernes) entre las 06:00 y las 18:00. La directiva usa la característica de administración de energía en el momento programado de la auditoría e intenta encender aquellas máquinas que estén apagadas antes de la auditoría. En general, se usa en situaciones en las que los clientes necesitan ejecutar auditorías durante los días de semana en horario laborable, ya que las máquinas suelen estar apagadas durante la noche y los fines de semana. La directiva puede aplicarse de forma selectiva a diversas máquinas, grupos de máquinas u organizaciones enteras de máquinas.

Vistas

Se proporciona un conjunto de vistas predefinidas que pueden usarse en todos los aspectos de la administración de servicios de TI y al brindar soporte al servicio de Auditoría/Inventario. Estas vistas permiten filtrar máquinas en todo el sistema sobre la base del hardware, el software y el rol. Las siguientes vistas se pueden usar tanto en la elaboración de informes como en las actividades operativas.

Nombre de la Vista	Descripción
zz[SYS] HW - Dell	Muestra todas las máquinas cuyo fabricante sea Dell.
zz[SYS] HW - Dell PowerEdge	Muestra todas las máquinas cuyo fabricante sea Dell y cuyo nombre de producto sea PowerEdge.
zz[SYS] HW - HP	Muestra todas las máquinas cuyo fabricante sea HP o Hewlett Packard.
zz[SYS] HW - HP ProLiant	Muestra todas las máquinas cuyo fabricante sea HP o Hewlett Packard y cuyo nombre de producto sea ProLiant.
zz[SYS] HW - IBM	Muestra todas las máquinas cuyo fabricante sea IBM.
zz[SYS] HW - IBM Series X	Muestra todas las máquinas cuyo fabricante sea IBM y cuyo nombre de producto sea Series X.
zz[SYS] HW - Lenovo	Muestra todas las máquinas cuyo fabricante sea Lenovo.
zz[SYS] HW - Not Portable	Muestra todas las máquinas que no son móviles.
zz[SYS] HW - Portable	Muestra todas las máquinas que son móviles (es decir, aquellas cuyo tipo de chasis sea un equipo portátil ligero, un equipo portátil regular, una Tablet PC, una computadora de bolsillo, una computadora miniportátil o una computadora ultraportátil).
zz[SYS] HW - Under 1GB Memory	Muestra todas las máquinas que tienen menos de 1 GB de memoria.
zz[SYS] HW - Under 512MB Memory	Muestra todas las máquinas que tienen menos de 512 MB de memoria.
zz[SYS] HW - Virtual Guest	Muestra todas las máquinas que son computadoras virtualizadas (invitados Hyper-V, VMWare, XenServer o VirtualBox).
zz[SYS] Network - 10.11.12.x	Muestra agentes de la red específica 10.11.12.x.
zz[SYS] OS - All Linux	Muestra todos los equipos Linux.
zz[SYS] OS - All Mac OS X	Muestra todas las máquinas Mac OS X.
zz[SYS] OS - All Mac OS X Servers	Muestra todas las máquinas con plataformas Mac OS X Server.
zz[SYS] OS - All Mac OS X Workstations	Muestra todas las máquinas con plataformas Mac OS X Workstation.
zz[SYS] OS - All Servers	Muestra todas las máquinas en las que se ejecuta un sistema operativo tipo servidor.
zz[SYS] OS - All Windows	Muestra todas las máquinas Windows.
zz[SYS] OS - All Windows SBS	Muestra todas las máquinas en las que se ejecuta el servidor Windows SBS.
zz[SYS] OS - All Windows Servers	Muestra todas las máquinas con Windows Server.
zz[SYS] OS - All Windows Workstations	Muestra todas las estaciones de trabajo Windows.
zz[SYS] OS - All Workstations	Muestra todas las máquinas en las que se ejecuta un sistema operativo tipo estación de trabajo.
zz[SYS] OS - Mac OS X 10.5 Leopard	Muestra todas las máquinas con Mac OS X v10.5.
zz[SYS] OS - Mac OS X 10.6 Snow Leopard	Muestra todas las máquinas con Mac OS X v10.6.
zz[SYS] OS - Mac OS X 10.7 Lion	Muestra todas las máquinas con Mac OS X v10.7.
zz[SYS] OS - Mac OS X 10.8 Mountain Lion	Muestra todas las máquinas con Mac OS X v10.8.

zz[SYS] OS - Win 2003 SBS	Muestra todas las máquinas en las que se ejecuta el sistema operativo Small Business Server de Windows 2003.
zz[SYS] OS - Win 2003 Server	Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows Server 2003.
zz[SYS] OS - Win 2008 R2 Server	Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows 2008 Server R2.
zz[SYS] OS - Win 2008 SBS	Muestra todas las máquinas en las que se ejecuta el sistema operativo Small Business Server de Windows 2008.
zz[SYS] OS - Win 2008 Server	Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows Server 2008.
zz[SYS] OS - Win 2012 Server	Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows Server 2012.
zz[SYS] OS - Win 7	Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows 7.
zz[SYS] OS - Win Vista	Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows Vista.
zz[SYS] OS - Win XP	Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows XP.
zz[SYS] Role - BackupExec Server	Muestra todos los servidores BackupExec.
zz[SYS] Role - Blackberry Server	Muestra todos los servidores Blackberry Enterprise.
zz[SYS] Role - BrightStor ARCserve Server	Muestra todos los servidores BrightStor ARCserve.
zz[SYS] Role - Citrix Server	Muestra todos los servidores Citrix.
zz[SYS] Role - DHCP Server	Muestra todos los servidores DHCP de MS.
zz[SYS] Role - DNS Server	Muestra todos los servidores DNS de MS.
zz[SYS] Role - Domain Controller	Muestra todos los servidores de controlador de dominio de AD de MS.
zz[SYS] Role - Exchange 2003 Server	Muestra todos los servidores MS Exchange 2003.
zz[SYS] Role - Exchange 2007 Server	Muestra todos los servidores MS Exchange 2007.
zz[SYS] Role - Exchange 2010 Server	Muestra todos los servidores MS Exchange 2010.
zz[SYS] Role - Exchange Server	Muestra todos los servidores MS Exchange.
zz[SYS] Role - File Server	Muestra todos los servidores de archivos de MS con recursos compartidos de archivos que no sean de administradores.
zz[SYS] Role - FTP Server	Muestra todos los servidores FTP de MS.
zz[SYS] Role - IIS Server	Muestra todos los servidores MS IIS.
zz[SYS] Role - IMAP4 Server	Muestra todos los servidores IMAP4 de MS.
zz[SYS] Role - POP3 Server	Muestra todos los servidores POP3 de MS.
zz[SYS] Role - Print Server	Muestra todos los servidores de impresión de MS con recursos compartidos de archivos que no sean de administradores.
zz[SYS] Role - SharePoint Server	Muestra todos los servidores SharePoint de MS.
zz[SYS] Role - SMTP Server	Muestra todos los servidores SMTP de MS que no sean a su vez servidores MS Exchange.
zz[SYS] Role - SQL Server	Muestra todos los servidores MS SQL Server.
zz[SYS] Role - SQL Server (Default Instance)	Muestra todos los servidores MS SQL configurados con la instancia predeterminada.
zz[SYS] Role - SQL Server 2005	Muestra todos los servidores MS SQL Server 2005.
zz[SYS] Role - SQL Server 2008	Muestra todos los servidores MS SQL Server 2008.
zz[SYS] Role - Terminal Server	Muestra todos los servidores Terminal Server de MS en modo de aplicación.

zz[SYS] Role - WINS Server	Muestra todos los servidores WINS de MS.

Administración de parches/actualizaciones

Objetivo

Proporcionar una estrategia de administración de parches y actualizaciones de rutina, a fin de que las máquinas administradas incluyan análisis y aplicación de parches, directivas de aprobación de parches, control sobre el comportamiento de los parches y visibilidad del estado y el cumplimiento de los parches que respalden la toma de decisiones y faciliten la solución de problemas.

Introducción

La administración de parches de Kaseya sólo es compatible con la aplicación de parches de Microsoft Windows. El estado de los parches de una máquina se detecta por medio de una detección de parches, y la implementación de estos se logra con la programación de una actualización automática, inicial, de máquinas o de parches. Una detección de parches permite detectar los parches faltantes e instalados en una máquina con el objetivo de poder tomar decisiones acerca de cómo proseguir con la estrategia de aplicación de parches. Los parches que se detectan mediante un análisis se presentan en un conjunto de directivas de parches que luego puede utilizarse para controlar qué parches están aprobados para ser implementados en las máquinas. Las actualizaciones automáticas implementan en las máquinas los parches aprobados de acuerdo con una programación y según la pertenencia a la directiva de parches. Las actualizaciones iniciales, de máquinas y de parches proporcionan capacidades de programación por única vez o manuales a la estrategia general de parches. A fin de contar con información actualizada disponible acerca del estado de los parches de las máquinas y así poder tomar decisiones sobre la implementación y aprobación relacionadas con los parches, es importante programar las auditorías de exploraciones de parches para que se ejecuten de acuerdo con un patrón regular periódico. La implementación regular de parches también es esencial para alcanzar los objetivos de la administración de parches; por lo tanto, es de igual importancia la programación de actualizaciones automáticas. Estas tareas periódicas pueden programarse con el contenido de la administración de parches. Este contenido también incluye un conjunto de directivas de parches a las cuales se pueden asignar diferentes máquinas, ya sea de forma automática o manual. Junto con esta estrategia de administración de parches, deben existir modos simples de ubicar sistemas específicos basados en los detalles de los parches instalados o faltantes, la cantidad de parches faltantes y las máquinas con determinadas directivas de parches. También deben existir modos de elaborar informes sobre estos grupos de máquinas, en caso de que sea necesario, y actuar de manera efectiva con respecto a ellos. El contenido adicional proporcionado con el paquete ofrece soporte básico para actualizaciones de software de Macintosh y de paquetes Linux.

Políticas

Se proporciona un conjunto de directivas que aplican programaciones periódicas de detección de parches y de actualizaciones automáticas en todas las máquinas que ejecutan Windows dentro de la infraestructura de TI a las que se les brinda soporte. Estas directivas permiten la detección periódica de parches instalados o faltantes en todas las máquinas, así como la programación de la implementación de los parches aprobados. Asimismo, se incluyen directivas para asignar servidores y estaciones de trabajo Windows a las directivas de parches adecuadas y para permitir que no se apliquen parches en determinadas máquinas, o para que se establezca un grupo de prueba en el cual implementar parches antes de la aprobación general e implementación de parches nuevos. Se proporciona una directiva adicional que aplica programaciones periódicas de actualizaciones de software de Macintosh en las máquinas con este sistema operativo dentro de la infraestructura de TI a las que se les brinda soporte.

Las directivas incluidas se encuentran en **[System].Core.Org Specific Policies.Patch / Update Management**, y se describen a continuación.

- **Windows.Common Windows Patch Mgmt Settings**
  - **Deny Patch Settings**: aplica ajustes de administración de parches a las máquinas seleccionadas en la vista 'zz[SYS] Policy - Patch_Deny Patching Group'. Establece la Acción de reinicio en “No reiniciar después de la actualización”. Establece la pertenencia a la directiva de parches en la directiva de parches “Deny Patching”. Establece las alertas de parches de manera que se genere una alarma y se envíe un correo electrónico a la dirección de alertas de parches cuando se produce un error en la instalación de un parche o cuando la credencial de agente no es válida o falta.
  - **Test Patch Settings**: aplica ajustes de administración de parches a las máquinas seleccionadas en la vista 'zz[SYS] Policy - Patch_Test Patching Group'. Establece la Acción de reinicio en “Si el usuario inició sesión, solicitarle que reinicie cada 60 minutos hasta que se produzca el reinicio. Reiniciar si el usuario no inició sesión”. Establece la pertenencia a la directiva de parches en la directiva de parches “Test Patching”. Establece las alertas de parches de manera que se genere una alarma y se envíe un correo electrónico a la dirección de alertas de parches cuando se produce un error en la instalación de un parche o cuando la credencial de agente no es válida o falta.
  - **Disable Windows Automatic Update**: deshabilita las actualizaciones automáticas de Windows en las máquinas que tienen habilitada la actualización automática de Windows. Si la actualización automática de Windows está habilitada y la administración de parches de Kaseya está en uso, dicha actualización puede entrar en conflicto con la estrategia de administración de parches de Kaseya, y esto puede derivar en la implementación de parches denegados o que aún no fueron aprobados por Kaseya.
  - **File Source Internet**: establece el Origen de archivo para la administración de parches en Internet para todos los equipos Windows de manera que los parches se descarguen directamente de los servidores de descarga y parches de Microsoft. Esta es la directiva predeterminada, y puede ser sustituida por una directiva alternativa que se aplique a determinadas organizaciones o grupos de máquinas y que tenga precedencia sobre esta directiva.
- **Windows.Windows Workstation Patch Mgmt Settings**
  - **Workstation Patch Settings**: aplica ajustes de administración de parches a las estaciones de trabajo Windows. Establece la Acción de reinicio en “Si el usuario inició sesión, solicitarle que reinicie cada 60 minutos hasta que se produzca el reinicio. Reiniciar si el usuario no inició sesión”. Establece la pertenencia a la directiva de parches en la directiva de parches “Workstation Patching”. Establece las alertas de parches de manera que se genere una alarma y se envíe un correo electrónico a la dirección de alertas de parches cuando se produce un error en la instalación de un parche o cuando la credencial de agente no es válida o falta.
  - **Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6am-6pm/Power Mgmt)**: aplica programaciones de actualizaciones automáticas diarias a los miembros de la directiva Workstation Patching a los que les falten 10 o más parches aprobados. Las actualizaciones automáticas se programan para llevarse a cabo de lunes a viernes, todas las semanas, entre las 06:00 y las 18:00. Esta directiva suele utilizarse cuando los clientes tienen máquinas a las que les faltan algunos pocos parches y desean actualizar esos sistemas en el transcurso de algunos días, en lugar de tener que esperar semanas o meses. Una vez que se instalan parches en las máquinas, ya no es necesario volver a hacerlo a diario. Las actualizaciones automáticas se llevan a cabo durante el día en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.
  - **Weekly Wkst Schedule (Scan Tu 6am-6pm/Auto Update W 6am-6pm/Power Mgmt)**: aplica programaciones semanales de detección de parches y actualizaciones automáticas a los miembros de la directiva Workstation Patching. Las detecciones de parches se programan para llevarse a cabo los martes de cada semana de 06:00 a 18:00 y las actualizaciones automáticas, los miércoles de cada semana en la misma franja horaria. Esta directiva suele

utilizarse cuando los clientes desean adoptar un enfoque más agresivo en lo que respecta a la aplicación parches, a fin de minimizar los riesgos derivados de la falta de estos en las máquinas, y, por ese motivo, quieren que los parches nuevos se instalen relativamente rápido en las máquinas. Las actualizaciones automáticas se llevan a cabo durante el día en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.

- **Windows.Windows Server Patch Mgmt Settings**
  - **Server Patch Settings**: aplica ajustes de administración de parches a los servidores Windows. Establece la Acción de reinicio en "No reiniciar después de la actualización", "Cuando se requiera reiniciar, enviar correo electrónico a la dirección de alertas de parches". Establece la pertenencia a la directiva de parches en la directiva de parches "Server Patching". Establece las alertas de parches de manera que se genere una alarma y se envíe un correo electrónico a la dirección de alertas de parches cuando se produce un error en la instalación de un parche o cuando la credencial de agente no es válida o falta.
  - **Weekly Srvr Schedule (Scan W 6pm-6am)**: aplica una programación de detección de parches a los miembros de la directiva de parches de servidores. Las detecciones de parches se programan para llevarse a cabo los miércoles de cada semana de 18:00 a 06:00. Según esta directiva, no se programan implementaciones de actualizaciones automáticas de parches.
- **Macintosh.Macintosh Workstation Software Update Settings**
  - **Weekly Macintosh Workstation Software Update (Install Recommended W 6pm-6am)**: aplica una actualización de software Mac para que se ejecute los miércoles de cada semana y por medio de la cual se instalan las actualizaciones de software Macintosh recomendadas en las estaciones de trabajo Macintosh. Las actualizaciones de software se llevan a cabo durante el día en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.

Directivas de aprobación y denegación de parches

Nota: Las directivas de aprobación y denegación de parches son un tipo específico de directiva del módulo de Administración de parches que no debe confundirse con las directivas definidas mediante el módulo **Policy Management**. Las directivas de **Policy Management** se crearon para especificar directivas predefinidas de aprobación y denegación de parches.

Se proporciona un conjunto de directivas de parches predefinidas para controlar la aprobación y denegación de diversos parches de Windows que se aplican al software compatible de Microsoft y a los sistemas operativos Windows.

Nombre de la política de parches	Descripción
zz[SYS] Deny Patching	Se usa para denegar todos los parches en aquellos casos en los que a las máquinas no se les debe aplicar parches por determinados motivos. El Estado de aprobación predeterminado de los parches nuevos de todas las clasificaciones de seguridad de Microsoft se establece en Denegado. Para obtener más información acerca del modo en que se pueden asignar máquinas a esta directiva de parches, consulte la Administración de pertenencia a la directiva de parches.
zz[SYS] Server Patching	Se usa para aprobar y denegar parches en los servidores Windows. El Estado de aprobación predeterminado de los parches nuevos de todas las clasificaciones de seguridad de Microsoft se establece en Pendiente de

	aprobación. Todos los servidores Windows pasan a integrar esta directiva de parches cuando la Administración de parches de servidores se habilita mediante la Administración automatizada de sistemas.
zz[SYS] Test Patching	Se usa para aprobar y denegar parches en máquinas destinadas a la prueba de parches antes de una implementación general en los servidores y estaciones de trabajo Windows. El Estado de aprobación predeterminado de las actualizaciones críticas y de seguridad de prioridad alta nuevas según las clasificaciones de seguridad de Microsoft se establece en Aprobado. Todos los servidores Windows pasan a integrar esta directiva de parches cuando la Administración de parches de servidores se habilita mediante la Administración automatizada de sistemas. Para obtener más información acerca del modo en que se pueden asignar máquinas a esta directiva de parches, consulte la Administración de pertenencia a la directiva de parches.
zz[SYS] Workstation Patching	Se usa para aprobar y denegar parches en las estaciones de trabajo Windows. El Estado de aprobación predeterminado de las actualizaciones críticas y de seguridad de prioridad alta nuevas según las clasificaciones de seguridad de Microsoft se establece en Aprobado. Todas las estaciones de trabajo Windows pasan a integrar esta directiva de parches cuando la Administración de parches de estaciones de trabajo se habilita mediante la Administración automatizada de sistemas.

Vistas

Se proporciona un conjunto de vistas predefinidas que pueden usarse en todos los aspectos de la administración de servicios de TI y al brindar soporte al servicio de administración de parches y actualizaciones. Estas vistas permiten filtrar máquinas en todo el sistema sobre la base de la configuración de parches, la cantidad de parches faltantes, el estado de reinicio por instalación de parches y la pertenencia a la directiva de parches, entre otros. Las siguientes vistas se pueden usar tanto en la elaboración de informes como en las actividades operativas.

Nombre de la Vista	Descripción
zz[SYS] Patch - Deny Patching Policy	Muestra todas las máquinas asignadas como miembros de la directiva de parches “zz[SYS] - Deny Patching”.
zz[SYS] Patch - Missing 10+ Approved Patches	Muestra todas las máquinas a las que les faltan 10 o más parches aprobados de acuerdo con la pertenencia a la directiva de parches de las máquinas y los parches aprobados dentro de esas directivas.
zz[SYS] Patch - Missing 20+ Approved Patches	Muestra todas las máquinas a las que les faltan 20 o más parches aprobados de acuerdo con la pertenencia a la directiva de parches de las máquinas y los parches aprobados dentro de esas directivas.
zz[SYS] Patch - No Policy	Muestra todas las máquinas que no están asignadas a ninguna directiva de parches.
zz[SYS] Patch - Pending Reboot	Muestra todas las máquinas con un reinicio pendiente relacionado con la implementación de parches.
zz[SYS] Patch - Scan Failed	Muestra todas las máquinas en las que, por algún motivo, se produjo un error en la última detección de parches.
zz[SYS] Patch - Scan Not Scheduled	Muestra todas las máquinas que no tienen programada una detección de parches.
zz[SYS] Patch - Server Patching Policy	Muestra todas las máquinas que pertenecen a la directiva de parches “zz[SYS] - Server Patching”.
zz[SYS] Patch - Servers w No Policy	Muestra todas las máquinas servidor que no están asignadas a ninguna directiva de parches.
zz[SYS] Patch - Test Patching Policy	Muestra todas las máquinas que pertenecen a la directiva de parches “zz[SYS] - Test Patching”.

zz[SYS] Patch - Windows Auto Update Enabled	Muestra todas las máquinas con la Actualización automática de Windows habilitada de acuerdo con lo detectado durante la última detección de parches.
zz[SYS] Patch - Workstation Patching Policy	Muestra todas las máquinas que pertenecen a la directiva de parches “zz[SYS] - Workstation Patching”.
zz[SYS] Patch - Workstations w No Policy	Muestra todas las estaciones de trabajo que no están asignadas a ninguna directiva de parches.

Procedimientos del Agente

Los procedimientos de agente se proporcionan para realizar automatizaciones personalizadas al brindar soporte al servicio de TI de administración de parches y actualizaciones. Estos procedimientos se encuentran en el gabinete **Sistema** de la página **Programar/Crear** *(http://help.kaseya.com/webhelp/ES/VSA/R8/index.asp#2845.htm)*, en Procedimientos de agente.

- **Create Patch Management System Restore Point**: ejecuta un procedimiento previo para las actualizaciones automáticas. Los puntos de restauración se pueden usar durante una recuperación en el caso de que la instalación de un parche o una actualización generen problemas.
  - **Ubicación:** System.Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore.Create Patch Management System Restore Point
  - **Descripción:** usa WMIC para crear un punto de restauración del sistema llamado Administración de parches. Se puede recurrir a este procedimiento de agente antes de la implementación de un parche por medio de un Procedimiento previo de agente para actualización automática.
  - **Ejecutado por directiva:** System.Core.Org Specific Policies.Patch/Update Management.Windows Workstation Patch Settings.Workstation Patch Settings
- **Mac Software Update - Install Recommended Updates and Retrieve/Log Results**
  - **Ubicación:** System.Core.2 Macintosh Procedures.Software Update.Mac Software Update - Install Recommended Updates and Retrieve/Log Results
  - **Descripción:** instala actualizaciones recomendadas de software Mac.
  - **Ejecutado por directiva:** System.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Workstation Software Update Settings.Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6pm-6am)

Mantenimiento de rutina

Objetivo

Proporcionar una estrategia de mantenimiento de rutina para que las máquinas administradas incluyan la optimización del sistema. A su vez, permitir operaciones de mantenimiento preventivo, tales como limpieza de discos y archivos temporales, análisis de unidad de disco duro, reparación y optimización, entre otras. El mantenimiento de rutina es fundamental para garantizar que los sistemas se ejecuten sin problemas y que funcionen al máximo de su potencial de rendimiento. Establezca una programación de mantenimiento básico de rutina automatizado en los sistemas a los que se les brinda soporte. En primer lugar, céntrese en las estaciones de trabajo, pero contemple la posibilidad de extenderse y brindar soporte a operaciones de mantenimiento más avanzadas y servidores (según sea necesario) con el pasar del tiempo.

Introducción

La automatización de Kaseya denominada “Procedimientos de agente” se puede usar para llevar a cabo la mayoría de las tareas automatizadas, en uno o más sistemas, de manera programada. Las tareas automáticas, tales como las verificaciones de discos, el análisis y la optimización de la desfragmentación de los discos, las reparaciones del volumen, la limpieza general, la eliminación de la

memoria caché, la limpieza de archivos temporales, la rotación de registros, entre otros, se combinan para formar una solución de mantenimiento de rutina eficaz que se aplica a las estaciones de trabajo Windows y Macintosh para mantener estos sistemas funcionando con fluidez.

Políticas

Un conjunto de directivas aplica programaciones de mantenimiento de rutina periódico en todas las estaciones de trabajo Windows y Macintosh. A su vez, estas directivas hacen que los procedimientos de agente efectúen el mantenimiento en cada sistema en momentos programados regularmente. Las directivas se encuentran en **[System].Core.Org Specific Policies.Routine Maintenance**, y se describen a continuación.

- **Windows Workstation Recurring Maintenance**
  - **Windows Workstation Maintenance (Weekly M-F 6pm-6am)**: aplica un procedimiento programado de mantenimiento de las estaciones de trabajo Windows que se ejecuta semanalmente en todas las estaciones de trabajo Windows, de lunes a viernes, entre las 18:00 y las 06:00. Si la máquina no está encendida en el momento en el cual está programado el mantenimiento, la máquina omitirá ese ciclo de mantenimiento e intentará ejecutarlo de nuevo una semana después.
- **Macintosh Workstation Recurring Maintenance**
  - **Macintosh Workstation Maintenance Schedule (Weekly M-F 6pm-6am)**: aplica un procedimiento programado de mantenimiento de las estaciones de trabajo Macintosh que se ejecuta semanalmente en todas las estaciones de trabajo Macintosh, de lunes a viernes, entre las 18:00 y las 06:00. Si la máquina no está encendida en el momento en el cual está programado el mantenimiento, la máquina omitirá ese ciclo de mantenimiento e intentará ejecutarlo de nuevo una semana después.

Procedimientos del Agente

Un conjunto de Procedimientos de agente lleva a cabo diversos aspectos de las tareas de mantenimiento en las estaciones de trabajo Windows y Macintosh. Estos procedimientos se programan por medio de una directiva que se ejecuta en forma periódica. Los procedimientos de agente se encuentran en **[System].Core**, , y se describen a continuación.

- **1 Windows Procedures.Desktops.Maintenance.Desktop Maintenance.Workstation Weekly Maintenance**
  - **Descripción:** ejecuta todas las tareas de mantenimiento semanal de escritorio; programe este script para que se ejecute durante el período de mantenimiento.
  - **Uso:** programado mediante la Administración de directivas para ejecutarse semanalmente (de lunes a viernes) en todas las estaciones de trabajo Windows, entre las 18:00 y las 06:00, por medio de la directiva Windows Workstation Maintenance (Weekly M-F 6pm-6am), siempre que la característica Mantenimiento de estaciones de trabajo esté habilitada mediante la Administración automatizada de sistemas.
- **Common Maintenance Tasks.System Restore.Create Weekly Desktop Maintenance System Restore Point**
  - **Descripción:** usa WMIC para crear un punto de restauración del sistema llamado Mantenimiento semanal de escritorio. Es posible recurrir a este procedimiento de agente al principio del Procedimiento de mantenimiento semanal de estaciones de trabajo.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de estaciones de trabajo.
- **Common Maintenance Tasks.Flush DNS. Flush DNS Resolver Cache**
  - **Descripción:** vacía y restablece el contenido de la memoria caché de resolución de clientes DNS ejecutando IPCONFIG /FLUSHDNS.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de estaciones de trabajo.
- **Common Maintenance Tasks.IE Files Management. Clear Internet Explorer Temp Files**
  - **Descripción:** borra los archivos temporales de Internet Explorer correspondientes al usuario que está conectado.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de estaciones de trabajo.

- **Common Maintenance Tasks.TEMP Files.Clear User TEMP Folder**
  - **Descripción:** elimina todos los archivos y carpetas dentro de la carpeta %TEMP% de los usuarios que iniciaron sesión que no se encuentran actualmente abiertos o bloqueados por Windows.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de estaciones de trabajo.
- **Common Maintenance Tasks.Disk Cleanup.Windows Disk Cleanup**
  - **Descripción:** establece las entradas de registro “sageset” para cleanmgr.exe y, a continuación, ejecuta cleanmgr.exe con el parámetro “sagerun” para que borre automáticamente los archivos en las ubicaciones siguientes: Carpeta temporal de configuración activa, Limpiador indexador de contenido, Archivos de programas descargados, Archivos caché de Internet, Archivos de volcado de memoria, Archivos ChkDsk antiguos, Papelera de reciclaje, Archivos caché de escritorio remotos, Archivos de registro de configuración, Archivos temporales, Archivos temporales sin conexión, Memoria caché de WebClient y WebPublisher.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de estaciones de trabajo.
- **Common Maintenance Tasks.Check Disk.Check Disk System Drive (Schedule at Next Restart)**
  - **Descripción:** ejecuta un comando CHKDSK en la unidad del sistema. Los resultados del mantenimiento se evalúan por medio del script Check Disk Verify.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de estaciones de trabajo.
- **Common Maintenance Tasks.Defragmentation.Defragment System Drive (Analysis & Prompt User If Reqd)**
  - **Descripción:** realiza un análisis de desfragmentación en la unidad del sistema en Windows (en general, en la unidad C:). Los resultados de la desfragmentación se escriben en el registro de procedimientos de agente. Si un usuario inició sesión en la máquina, el procedimiento brinda la opción de ejecutar una desfragmentación completa en la unidad y la lleva a cabo si se el usuario responde afirmativamente.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de estaciones de trabajo.
- **2 Macintosh Procedures.Maintenance.Macintosh Weekly Maintenance**
  - **Descripción:** realiza una serie de tareas de mantenimiento de rutina en una máquina con Macintosh OS X.
  - **Uso:** programado mediante la Administración de directivas para ejecutarse semanalmente (de lunes a viernes) en todas las estaciones de trabajo Macintosh, entre las 18:00 y las 06:00, por medio de la directiva Macintosh Workstation Maintenance Schedule (Weekly M-F 6pm-6am), siempre que la característica Mantenimiento de estaciones de trabajo esté habilitada mediante la Administración automatizada de sistemas.
- **General OS X House Cleaning**
  - **Descripción:** realiza una limpieza del sistema, elimina archivos de registro antiguos, archivos de trabajo y archivos basura, limpia las memorias caché de los usuarios y del sistema, rota los registros del sistema y de aplicaciones, y vuelve a generar la memoria caché DYLD y el índice Spotlight.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de Macintosh.
- **Verify and Repair OS X Disk Volumes**
  - **Descripción:** lleva a cabo operaciones de verificación y reparación de disco con DISKUTIL.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de Macintosh.
- **Repair OS X Disk Permissions**
  - **Descripción:** lleva a cabo una operación de permisos de reparación de disco con DISKUTIL.
  - **Uso:** lo invoca el Procedimiento de mantenimiento semanal de Macintosh.

Monitoreo

En esta sección

Introducción a las funciones de supervisión

Objetivo

Proporcionar una estrategia de supervisión para controlar los activos de hardware y software, y enviar alertas relacionadas con estos. La supervisión constante de los eventos críticos del sistema en los servidores Windows, durante los siete días de la semana, garantiza el buen estado de la infraestructura de TI. En caso de que ocurra un problema, la continuidad de su negocio podría sufrir un impacto sustancial si no fuera notificado de forma inmediata. A medida que se realizan cambios en las máquinas que se encuentran dentro de la infraestructura de TI a la cual se le brinda soporte, la supervisión debe ir captando esos cambios para poder tenerlos en cuenta y así llevarse a cabo de manera adecuada.

Introducción

La supervisión de Kaseya proporciona varias maneras de controlar sistemas basados en agentes y sistemas que no se basan en ellos, dentro de una infraestructura de TI de clientes a la cual se le brinda soporte. La supervisión de disponibilidad del servidor en forma de alertas de estado del agente genera notificaciones ante una caída de los sistemas o ante su desconexión por causas principales como bloqueos, reinicios, conectividad de la red, sobrecarga del sistema, etc. La supervisión del Servicio de Windows en forma de conjuntos de monitores con comprobaciones de servicios proporciona una supervisión continua de los Servicios de Windows importantes. También envía notificaciones y realiza correcciones automáticas (servicios de reinicio) cuando estos servicios no están en ejecución o están detenidos. La supervisión de registros de eventos en forma de alertas de conjuntos de eventos proporciona una supervisión continua de los Registros de eventos de Windows y envía notificaciones cuando se registran eventos importantes en dichos registros. La supervisión del rendimiento en forma de conjuntos de monitores con umbrales del contador proporciona una supervisión continua de los contadores de rendimiento de Windows y envía notificaciones cuando los valores de los contadores alcanzan determinados umbrales que podrían tener un impacto negativo en el rendimiento del sistema, la disponibilidad o la confiabilidad de este. Los estados de supervisión, eventos y valores de los contadores se registran en el sistema con el propósito de actualizar datos históricos, tendencias e informes. Las alarmas que generan los sistemas de supervisión se registran en el sistema con fines históricos y de elaboración de informes. Se admiten varios niveles de gravedad de manera que los problemas que surjan puedan priorizarse de manera adecuada y se envíen notificaciones a las personas correctas por correo electrónico.

En la siguiente Introducción a las funciones de supervisión, se muestran los tipos de sistemas y supervisión que se incluyen en el paquete de soluciones estándar.

Tipos de supervisión = (A = Disponibilidad, E = Registro de evento, S = Servicios, P = Rendimiento)

Tipo de sistema (categoría)	Tipos de supervisión	Información general de supervisión
Todos los servidores Windows (SO)	AESP	Supervisión de servicios básicos de servidores Windows
Windows Server 2003 (SO)	--S-	Servicios Windows 2003
Windows Server 2008/2008 R2 (SO)	--S-	Servicios Windows 2008/2008R2

Todas la estaciones de trabajo Windows (SO)	AESP	Supervisión de servicios básicos de estaciones de trabajo Windows
Windows Vista (SO)	--S-	Servicios Windows Vista
Windows 7 (SO)	--S-	Servicios Windows 7
Windows XP (SO)	--S-	Servicios Windows XP
Dell PowerEdge (hardware)	-E--	Eventos de hardware en Dell PowerEdge
HP ProLiant (hardware)	-E--	Eventos de hardware en HP ProLiant
IBM Series x (hardware del servidor)	-E--	Eventos de hardware en IBM Series x
Servidor Backup Exec (rol)	-ES-	Supervisión de Backup Exec
Servidor Blackberry Enterprise	-ESP	Supervisión del servidor Blackberry
Servidor BrightStor ARCServe	-ES-	Supervisión del servidor BrightStor
Servidor Citrix	-ES-	Supervisión del servidor Citrix
Servidor DHCP	-ESP	Supervisión del servidor DHCP
Servidor DNS	-ESP	Supervisión del servidor DNS
Controlador de dominio (infraestructura de red)	-ESP	Supervisión de controlador de dominio de AD
Servidor Exchange 2003 (correo electrónico)	-ES-	Supervisión de Exchange 2003
Servidor Exchange 2007 (correo electrónico)	-ES-	Supervisión de Exchange 2007
Servidor Exchange 2010 (correo electrónico)	-ESP	Supervisión de Exchange 2010
Servidor Exchange (correo electrónico)	-ESP	Supervisión de servicios básicos de Exchange
Servidor de archivos (Archivo/Impresión)	--S-	Supervisión de servidor de archivos
Servidor FTP (sistemas web)	--S-	Supervisión del servidor FTP
Servidor IIS (sistemas web)	-ESP	Supervisión del servidor IIS
Servidor IMAP4 (correo electrónico)	--S-	Supervisión del servidor IMAP4
Servidor POP3 (correo electrónico)	--S-	Supervisión del servidor POP3
Servidor de impresión (Archivo/Impresión)	-ESP	Supervisión del servidor de impresión
Microsoft SE-FEP (seguridad)	-ES-	Supervisión de Microsoft SE-FEP
Servidor SharePoint (sistemas web)	--S-	Supervisión del servidor SharePoint
Servidor SMTP (correo electrónico)	-ESP	Supervisión del servidor SMTP
SQL Server (base de datos)	--SP	Supervisión de servicios básicos de SQL Server
SQL Server 2005 (base de datos)	--S-	Supervisión de SQL Server 2005
SQL Server 2008 (base de datos)	--S-	Supervisión de SQL Server 2008
Terminal Server (acceso remoto)	-ESP	Supervisión de Terminal Server
Servidor WINS (infraestructura de red)	--S-	Supervisión del servidor WINS
AVG Technologies (seguridad)	--S-	Supervisión de antivirus AVG Technologies
Kaspersky ES (seguridad)	--S-	Supervisión de Kaspersky ES
McAfee (seguridad)	-ES-	Supervisión de McAfee
Sophos (seguridad)	-ES-	Supervisión de Sophos
Antivirus Symantec (seguridad)	-ES-	Supervisión de antivirus Symantec
Symantec EP (seguridad)	-ES-	Supervisión de antivirus McAfee
Trend Micro (seguridad)	-ES-	Supervisión de antivirus McAfee

Supervisión de la matriz de gravedad

		Acciones de supervisión		
Nivel de gravedad	**Descripción**	**Correo Electrónico**	**Tendencia**	**Rearmar**
Severity0	Informativo/registro	No	No	N/D
Severity1	Impacto/riesgo bajo	Sí	Sí	7 días
Severity2	Impacto/riesgo medio	Sí	Sí	1 Días
Severity3	Impacto/riesgo alto	Sí	Sí	12 horas
Alerta fija	Impacto/riesgo alto	Sí	Sí	12 horas

Nota: Los niveles de gravedad sólo se aplican a los conjuntos de monitores y de eventos y se designan en el nombre del conjunto. Todas las alertas fijas están configuradas para funcionar como nivel de Gravedad 3.

Directivas de supervisión

Existe un conjunto de directivas que aplica ajustes específicos de *supervisión* a las máquinas sobre la base del sistema operativo Windows y su versión, hardware, rol funcional y productos de seguridad o antivirus. Estas directivas habilitan los diversos componentes de supervisión (disponibilidad, registro de eventos, servicio y rendimiento) y su automatización. Las directivas se encuentran en **[System].Core.Org Specific Policies.Monitoring**, , y se describen a continuación.

En esta sección

Servidor

- **Common Windows Server Monitoring**: aplica un conjunto común de tareas de supervisión a todos los servidores Windows Server. Esto incluye la supervisión de los registros de eventos relacionados con el hardware, el Servicio de Windows y el rendimiento común de Windows.
- **Windows Server (Core)**: aplica un conjunto de ajustes de supervisión de servicios básicos de Windows Server, en el que se incluyen la supervisión de servicios estándar, del rendimiento del sistema, de la elaboración de informes de estado y de los registros de eventos, entre otros.
- **Windows Server 2003**: aplica ajustes de supervisión de servicio estándar para servidores Windows Server 2003.
- **Windows Server 2008/2008 R2**: aplica ajustes de supervisión de servicio estándar para servidores Windows Server 2008/2008 R2.

Hardware

- **Dell PowerEdge**: aplica ajustes de supervisión y alerta específicos del hardware de servidores Dell PowerEdge. Es posible que este tipo de supervisión requiera la instalación de herramientas de administración específicas de los servidores Dell PowerEdge en la máquina servidor.
- **HP ProLiant**: aplica ajustes de supervisión y alerta específicos del hardware de servidores HP ProLiant. Es posible que este tipo de supervisión requiera la instalación de herramientas de administración específicas de los servidores HP ProLiant en la máquina servidor.
- **IBM Series x**: aplica ajustes de supervisión y alerta específicos del hardware de servidores IBM Series X. Es posible que este tipo de supervisión requiera la instalación de herramientas de administración específicas de los servidores IBM Series X en la máquina servidor.

Roles

- **Backup Exec Server**: aplica ajustes de supervisión a servidores Backup Exec.
- **Blackberry Enterprise Server**: aplica ajustes de supervisión a servidores Blackberry Enterprise Server.
- **BrightStor ARCServe Server**: aplica ajustes de supervisión a servidores BrightStor.
- **Citrix Server**: aplica ajustes de supervisión a servidores Citrix.
- **DHCP Server**: aplica ajustes de supervisión a servidores DHCP.
- **DNS Server**: aplica ajustes de supervisión a servidores DNS.
- **Domain Controller**: aplica ajustes de supervisión a los controladores de dominio.

- **Exchange Server 2003**: aplica ajustes de supervisión a servidores Exchange 2003.
- **Exchange Server 2007**: aplica ajustes de supervisión a servidores Exchange 2007.
- **Exchange Server 2010**: aplica ajustes de supervisión a servidores Exchange 2010.
- **Exchange Server**: aplica ajustes de supervisión a servidores Exchange.
- **File Server**: aplica ajustes de supervisión a servidores de archivos.
- **FTP Server**: aplica ajustes de supervisión a servidores FTP.
- **IIS Server**: aplica ajustes de supervisión a servidores IIS.
- **IMAP4 Server**: aplica ajustes de supervisión a servidores IMAP4.
- **POP3 Server**: aplica ajustes de supervisión a servidores POP3.
- **Print Server**: aplica ajustes de supervisión a servidores de impresión.
- **SharePoint Server**: aplica ajustes de supervisión a servidores SharePoint.
- **SMTP Server**: aplica ajustes de supervisión a servidores SMTP.
- **SQL Server**: aplica ajustes de supervisión a servidores SQL.
- **SQL Server 2005**: aplica ajustes de supervisión a servidores SQL Server 2005.
- **SQL Server 2008**: aplica ajustes de supervisión a servidores SQL Server 2008.
- **Terminal Server**: aplica ajustes de supervisión a servidores Terminal Server.
- **WINS Server**: aplica ajustes de supervisión a servidores WINS.

Estación de Trabajo

- **Common Windows Workstation Monitoring**: aplica un conjunto común de ajustes de supervisión a todas las estaciones de trabajo Windows. Esto incluye la supervisión de los registros de eventos relacionados con el hardware, el Servicio de Windows y el rendimiento común de Windows.
- **Windows Workstation (Core)**: aplica un conjunto de ajustes de supervisión de servicios básicos de estaciones de trabajo Windows, en el que se incluyen la supervisión de servicios estándar, del rendimiento del sistema y de la elaboración de informes de estado, entre otros.
- **Windows Vista**: aplica ajustes de supervisión de servicio estándar para máquinas con Windows Vista.
- **Windows 7**: aplica ajustes de supervisión de servicio estándar para máquinas con Windows 7.
- **Windows XP**: aplica ajustes de supervisión de servicio estándar para máquinas con Windows XP.

Security.Antivirus

- **AVG Tech**: aplica ajustes de supervisión para los antivirus de AVG Technologies.
- **McAfee**: aplica ajustes de supervisión para los antivirus McAfee.
- **Microsoft SE-FEP**: aplica ajustes de supervisión para Microsoft Security Essentials y Forefront Endpoint Protection.
- **Sophos**: aplica ajustes de supervisión para los antivirus Sophos.
- **Symantec AV**: aplica ajustes de supervisión para los antivirus Symantec.
- **Symantec EP**: aplica ajustes de supervisión para los antivirus Symantec Endpoint Protection.
- **Trend Micro**: aplica ajustes de supervisión para los antivirus Trend Micro.

Utilidades

- **Update Lists By Scan**: programa una actualización de listas mediante análisis para que se ejecute en todas las máquinas Windows para mantener actualizada la información sobre el contador de rendimiento, el registro de eventos y los servicios en ejecución de cada máquina, a fin de lograr una supervisión precisa.
- **Monitoring Cleanup**: como última directiva con conjuntos de alertas y monitores, esta directiva garantiza de manera efectiva la eliminación de los ajustes de supervisión aplicados anteriormente (alertas de registros de eventos y conjuntos de monitores asignados por medio de otras directivas que ya no son necesarias debido a cambios de rol, etc.).

Conjuntos de Monitores

Se proporcionan y aplican varios conjuntos de monitores por medio de directivas relacionadas con la supervisión. Estos conjuntos de monitores supervisan los Servicios de Windows y los contadores de rendimiento por medio de verificaciones de servicios y umbrales del contador. Los conjuntos de monitores proporcionados incluyen ajustes de supervisión para servicios importantes del SO Windows y servicios para sistemas comunes de Microsoft, tales como Active Directory, Exchange, SQL, IIS, entre otros. Se incluyen ajustes básicos de supervisión de rendimiento del sistema para controlar el espacio en disco, el uso de memoria y el uso de CPU, así como ajustes específicos más avanzados. Los conjuntos de monitores se encuentran en **[System].Core**, y se describen a continuación.

En esta sección

Respaldo

- **Backup - Backup Exec Continuous Protection Services - {Severity3}**
  - Supervisa los servicios de protección continua de Backup Exec en los servidores Backup Exec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Backup - Backup Exec DLO Agent Services - {Severity3}**
  - Supervisa los servicios de agentes DLO de Backup Exec en los servidores Backup Exec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Backup - Backup Exec Services - {Severity3}**
  - Supervisa los servicios de Backup Exec en los servidores Backup Exec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Backup - Backup Exec System Recovery Service - {Severity3}**
  - Supervisa los servicios de recuperación del sistema de Backup Exec en los servidores Backup Exec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Backup - BrightStor ARCServe Backup Services - {Severity3}**
  - Supervisa los servicios de BrightStor ARCServe Backup en los servidores BrightStor ARCServe Backup. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Base de datos

- **Database - SQL Server (All Instances) Services - {Severity3}**

- Supervisa los servicios de SQL Server en los servidores SQL Server que usan el servicio de comodines MSSQL*. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

- **Database - SQL Server (Default Instance) - {Severity0}**
  - Recolecta contadores de rendimiento de SQL Server (instancia predeterminada) en los servidores SQL Server. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Database - SQL Server (Default Instance) Performance - {Severity2}**
  - Supervisa el rendimiento de SQL Server (instancia predeterminada) en los servidores SQL Server. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Database - SQL Server (Default Instance) Services - {Severity3}**
  - Supervisa los servicios de SQL Server (instancia predeterminada) en los servidores SQL Server. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Database - SQL Server 2005 Optional Services - {Severity3}**
  - Supervisa los servicios opcionales de SQL Server 2005 en los servidores SQL Server 2005. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Database - SQL Server 2005 Services - {Severity3}**
  - Supervisa los servicios de SQL Server 2005 en los servidores SQL Server 2005. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Database - SQL Server 2008 Optional Services - {Severity3}**
  - Supervisa los servicios opcionales de SQL Server 2008 en los servidores SQL Server 2008. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Database - SQL Server 2008 Services - {Severity3}**
  - Supervisa los servicios de SQL Server 2008 en los servidores SQL Server 2008. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Correo Electrónico

- **Email - Blackberry Server Performance - {Severity2}**
  - Supervisa el rendimiento del servidor Blackberry en los servidores Blackberry. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Email - BlackBerry Server Services - {Severity3}**
  - Supervisa los servicios del servidor Blackberry en los servidores Blackberry. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange 2003 Services - {Severity3}**
  - Supervisa los servicios de Exchange 2003 en los servidores Exchange 2003. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange 2007 Services - {Severity3}**
  - Supervisa los servicios de Exchange 2007 en los servidores Exchange 2007. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

- **Email - Exchange 2010 Edge Transport Queues - {Severity0}**
  - Recolecta contadores de rendimiento de colas de Exchange 2010 Edge Transport en servidores Exchange 2010. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity2}**
  - Supervisa el rendimiento de colas en Exchange 2010 Edge Transport en los servidores Exchange 2010. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity3}**
  - Supervisa el rendimiento de colas en Exchange 2010 Edge Transport en los servidores Exchange 2010. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange 2010 Services - {Severity3}**
  - Supervisa los servicios de Exchange 2010 en las máquinas Exchange 2010. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange Client Active Logons - {Severity0}**
  - Recolecta contadores de rendimiento de inicios de sesión activos de clientes Exchange en los servidores Exchange. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Email - Exchange IMAP4 Service - {Severity3}**
  - Supervisa el servicio Exchange IMAP4 en los servidores Exchange. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange POP3 Service - {Severity3}**
  - Supervisa el servicio Exchange POP3 en los servidores Exchange. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange Server (Core) Performance - {Severity2}**
  - Supervisa el rendimiento de Exchange Server en los servidores Exchange. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Email - Exchange Server (Core) Services - {Severity3}**
  - Supervisa los servicios de Exchange Server (básico) en las máquinas con servidor Exchange (básico). Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange Server (Core) Store and Database - {Severity0}**
  - Recolecta contadores de rendimiento de almacenamiento y base de datos de Exchange Server en los servidores Exchange. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Email - SMTP Queue Performance - {Severity3}**
  - Supervisa el rendimiento de colas SMTP en los servidores SMTP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - SMTP Server Service - {Severity3}**
  - Supervisa el servicio de servidor SMTP en los servidores SMTP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Archivo/impresión

- **File / Print - DFS Service - {Severity3}**
  - Supervisa el servicio DFS en las máquinas DFS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **File / Print - DFSR Service - {Severity3}**
  - Supervisa el servicio DFS en las máquinas DFSR. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **File / Print - NTFRS Service - {Severity3}**
  - Supervisa el servicio NTFRS en las máquinas NTFRS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **File / Print - Print Queue Job Errors Performance - {Severity1}**
  - Supervisa el rendimiento de errores en trabajos en colas de impresión en los servidores de archivos e impresión. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **File / Print - Spooler Service - {Severity3}**
  - Supervisa el servicio del administrador de trabajos en cola en los servidores de archivos e impresión. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Infraestructura de red

- **Network Infrastructure - Active Directory Domain Controller Services - {Severity3}**
  - Supervisa los servicios de controlador de dominio de Active Directory en los controladores de dominio de Active Directory. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Network Infrastructure - DHCP Server Performance - {Severity2}**
  - Supervisa el rendimiento del servidor DHCP en los servidores DHCP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Network Infrastructure - DHCP Server Service - {Severity3}**
  - Supervisa el servicio del servidor DHCP en los servidores DHCP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Network Infrastructure - DNS Server Performance - {Severity2}**
  - Supervisa el rendimiento del servidor DNS en los servidores DNS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Network Infrastructure - DNS Server Service - {Severity3}**
  - Supervisa el servicio del servidor DNS en los servidores DNS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Network Infrastructure - WINS Server Service - {Severity3}**
  - Supervisa el servicio del servidor WINS en los servidores WINS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

OS Platforms.Windows (Core).Disk Space

- **Windows (Core) - Free Disk Space on Drive C - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad C de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive D - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad D de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive E - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad E de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive F - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad F de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive G - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad G de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Space on C Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad C por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Space on D Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad D por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Space on E Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad E por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Space on F Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad F por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Space on G Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad G por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).

OS Platforms.Windows (Core)

- **Windows (Core) - All Automatic Services - {Severity0}**
  - Recolecta el estado del servicio de todos los servicios automáticos en las máquinas Windows. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Windows (Core) - CPU and Memory - {Severity0}**

  - Recolecta contadores de rendimiento de CPU y memoria en las máquinas Windows. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Windows (Core) - Free Disk Space on Any Drive Below 1GB - {Severity2}**
  - Supervisa el espacio libre en disco en cualquier unidad por debajo de 1 GB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Windows (Core) - Free Disk Space on Any Drive Below 2GB - {Severity1}**
  - Supervisa el espacio libre en disco en cualquier unidad por debajo de 2 GB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Disk Space on Any Drive Below 750MB - {Severity3}**
  - Supervisa el espacio libre en disco en cualquier unidad por debajo de 750 MB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive C Below 1GB - {Severity2}**
  - Supervisa el espacio libre en disco en la unidad C por debajo de 1 GB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Windows (Core) - Free Disk Space on Drive C Below 2GB - {Severity1}**
  - Supervisa el espacio libre en disco en la unidad C por debajo de 2 GB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Disk Space on Drive C Below 750MB - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad C por debajo de 750 MB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Machine Health - {Severity0}**
  - Recolecta contadores de rendimiento del estado de la máquina en las máquinas Windows. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Windows (Core) - Processor and Memory Performance - {Severity2}**
  - Supervisa el rendimiento del procesador y la memoria en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Windows (Core) - TCPv4 Connections Performance - {Severity2**}
  - Supervisa el rendimiento de las conexiones TCPv4 en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).

Plataformas de SO en servidores Windows

- **Windows Server (Core) - Cluster Services - {Severity3}**
  - Supervisa los servicios de clúster en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows Server (Core) - Disk Time and Queue Length Performance - {Severity2}**
  - Supervisa el rendimiento del tiempo de disco y la longitud de la cola en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Windows Server (Core) - Drive C Performance - {Severity1}**

- Supervisa el rendimiento de la unidad C en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).

- **Windows Server (Core) - General System Performance - {Severity1}**
  - Supervisa el rendimiento general del sistema en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows Server (Core) - Server Reboots - {Severity1}**
  - Supervisa los reinicios del servidor en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows Server (Core) - Standard Services - {Severity3}**
  - Supervisa los servicios estándar en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows Server 2003 - Standard Services - {Severity3}**
  - Supervisa los servicios estándar en las máquinas con Windows Server 2003. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows Server 2008/2008 R2 - Standard Services - {Severity3}**
  - Supervisa los servicios estándar en las máquinas con Windows Server 2008/2008 R2. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

OS Platforms.Windows Workstations

- **Windows 7 - Standard Services - {Severity1}**
  - Supervisa los servicios estándar en las máquinas con Windows 7. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows Vista - Standard Services - {Severity1}**
  - Supervisa los servicios estándar en las máquinas con Windows Vista. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows XP - Standard Services - {Severity1}**
  - Supervisa los servicios estándar en las máquinas con Windows XP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).

Acceso remoto

- **Remote Access - Citrix Licensing Service - {Severity3}**
  - Supervisa el servicio de licencia de Citrix en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Citrix Licensing WMI Service - {Severity3}**
  - Supervisa el servicio de licencia de Citrix WMI en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Citrix MetaFrame Services - {Severity3}**

- Supervisa los servicios Citrix MetaFrame en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

- **Remote Access - Citrix Server Services - {Severity3}**
  - Supervisa los servicios de los servidores Citrix en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Citrix Virtual Memory Optimization Service - {Severity3}**
  - Supervisa el servicio de optimización de memoria virtual Citrix en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Terminal Server Services - {Severity3}**
  - Supervisa los servicios de los servidores Terminal Server en los servidores Terminal Server. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Terminal Server Session Performance - {Severity2}**
  - Supervisa el rendimiento de sesión de los servidores Terminal Server en los servidores Terminal Server. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).

Pestaña de Seguridad

- **AV - AVG Tech AVG Services - {Severity3}**
  - Supervisa los servicios de AVG Technologies en las máquinas con protección AVG Technologies. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Kaspersky Endpoint Security Services {Severity3}**
  - Supervisa los servicios de Kaspersky Endpoint Security en las máquinas con protección Kaspersky Endpoint Security. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - McAfee Enterprise Services - {Severity3}**
  - Supervisa los servicios de McAfee Enterprise en las máquinas con protección McAfee Enterprise. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Sophos Antivirus Services - {Severity3}**
  - Supervisa los servicios de Sophos Antivirus en las máquinas con protección Sophos. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Symantec Antivirus Services - {Severity3}**
  - Supervisa los servicios de Symantec Antivirus en las máquinas con protección Symantec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Symantec Endpoint Protection Services - {Severity3}**
  - Supervisa los servicios de Symantec Endpoint Protection en las máquinas con protección Symantec Endpoint Protection. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Trend Micro Client Server Security Services - {Severity3}**
  - Supervisa los servicios Trend Micro Client/Server Security en las máquinas con protección Trend Micro Client/Server Security. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

- **AV - Trend Micro OfficeScan Services - {Severity3}**
  - Supervisa los servicios Trend Micro OfficeScan en las máquinas con protección Trend Micro OfficeScan. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Sistemas web

- **Web Systems - FTP Server Service - {Severity3}**
  - Supervisa el servicio del servidor FTP en los servidores FTP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Web Systems - IIS Performance - {Severity3}**
  - Supervisa el rendimiento de IIS en los servidores IIS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Web Systems - IIS Server - {Severity0}**
  - Recolecta contadores de rendimiento del servidor IIS en los servidores IIS. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Web Systems - IIS Server Services - {Severity3}**
  - Supervisa los servicios del servidor IIS en los servidores IIS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Web Systems - SharePoint Server Services - {Severity3}**
  - Supervisa los servicios del servidor SharePoint en los servidores SharePoint. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Conjuntos de Eventos

Se proporcionan y aplican varios conjuntos de eventos por medio de directivas relacionadas con la supervisión. Estos conjuntos de eventos supervisan los registros de eventos de Windows para determinados eventos. Los conjuntos de eventos proporcionados incluyen ajustes de supervisión para eventos importantes del SO Windows y servicios para sistemas comunes de Microsoft, tales como Active Directory, Exchange, SQL, IIS, sistemas y aplicaciones de terceros, entre otros. Los conjuntos de eventos incluidos se agruparon por categoría y se describen a continuación.

En esta sección

Pestaña de Seguridad

- **zz[SYS] AV - McAfee Anti-Virus (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de antivirus McAfee en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] AV - Microsoft SE-FEP (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de Microsoft Security Essentials y Forefront Endpoint Protection en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] AV - Misc AntiVirus (EW) - APP-SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de antivirus diversos en los registros de eventos de la aplicación y del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] AV - Misc AntiVirus (I) - APP-SYS - {Severity1}**
  - Supervisa eventos específicos de información de antivirus diversos en los registros de eventos de la aplicación y del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de antivirus Symantec y Norton en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de antivirus Symantec y Norton en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de antivirus Symantec y Norton en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).

- **zz[SYS] AV - Symantec/Norton AntiVirus (I) - APP - {Severity0}**
  - Supervisa eventos específicos de información de antivirus Symantec y Norton en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.

Respaldo

- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de Backup Exec en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de Backup Exec en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de Backup Exec en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Backup - Backup Exec (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de Backup Exec en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Backup - Backup Exec (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de Backup Exec en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Backup - Backup Exec Job Failure/Cancellation (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores por cancelaciones o errores de trabajo de Backup Exec en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Backup - Backup Exec Job Success (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de trabajos realizados correctamente de Backup Exec en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Backup - BrightStor ARCserve (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de BrightStor ARCserve en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Backup - BrightStor ARCServe (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de BrightStor ARCserve en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Backup - Microsoft Windows Backup (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de Microsoft Windows Backup en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Backup - Misc Backup (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores de copia de seguridad diversos en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Backup - Misc Backup (I) - APP - {Severity0}**
  - Supervisa eventos específicos de información de copia de seguridad diversos en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Backup - Misc Backup (W) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias de copia de seguridad diversas en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).

Base de datos

- **zz[SYS] Database - SQL Server (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de las características ACID de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de las características ACID de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de las características ACID de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - ACID (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de las características ACID de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de las copias de seguridad de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de las copias de seguridad de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - Backup (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de las copias de seguridad de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de los recursos de base de datos de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de los recursos de base de datos de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de los recursos de base de datos de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - DB Resources (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de los recursos de base de datos de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.

- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del MSDTC de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del MSDTC de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del MSDTC de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - MSDTC (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos del MSDTC de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de red de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de red de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de consultas de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de consultas de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de las replicaciones de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de las replicaciones de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de las replicaciones de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - Replication (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de las replicaciones de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de elaboración de informes de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de elaboración de informes de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Reporting (EWISFCV) - APP - {Severity0}**

- Supervisa eventos específicos de elaboración de informes de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.

- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de varias instancias del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de varias instancias del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de varias instancias del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de varias instancias del Agente SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de instancia única del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de instancia única del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de instancia única del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server Agent - Single Instance (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de instancia única del Agente SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server Cluster (I) - SYS - {Severity2}**
  - Supervisa eventos específicos de información de clúster de SQL Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL/Service Control Manager (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de SQL Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).

Correo Electrónico

- **zz[SYS] Email - Blackberry Server (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity2}**

- Supervisa eventos específicos de advertencias del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).

- **zz[SYS] Email - Blackberry Server Events (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de eventos del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Blackberry Server Events (W) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias de eventos del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2000 and 2003 (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores de Exchange 2000 y 2003 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2000 y 2003 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2000 y 2003 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2000 and 2003 and 2007 (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2000, 2003 y 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de Exchange 2007 en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de acceso de clientes de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de acceso de clientes de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de acceso de clientes de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Edge Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Edge Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Edge Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Hub Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Hub Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Hub Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de buzón de correo de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de buzón de correo de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de buzón de correo de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Mailbox (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de buzón de correo de Exchange 2007 en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de los servicios Transport de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de los servicios Transport de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de los servicios Transport de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity1}**

  - Supervisa eventos específicos de errores y advertencias del servicio de mensajería unificada de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias del servicio de mensajería unificada de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias del servicio de mensajería unificada de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2010 Server (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores del servidor Exchange 2010 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias del servidor Exchange 2010 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias del servidor Exchange 2010 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias del servidor Exchange 2010 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de Exchange Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de Exchange Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange Server (I) - SYS - {Severity3}**
  - Supervisa eventos específicos de información de Exchange Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange Server 5.5 (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de Exchange Server 5.5 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange/Service Control Manager (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de Exchange en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - SMTP/Service Control Manager (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de SMTP en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).

Hardware

- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de las baterías Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de las baterías Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de las baterías Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Battery (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de las baterías Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del controlador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del controlador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del controlador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Controller (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos del controlador de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores eléctricos de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores eléctricos de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores eléctricos de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Electrical (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos eléctricos específicos de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de gabinetes Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de gabinetes Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de gabinetes Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Enclosure (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de gabinetes Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de entorno de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de entorno de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de entorno de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Environmental (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de entorno de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del ventilador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del ventilador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del ventilador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Fan (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos del ventilador de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con cambios en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con cambios en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores relacionados con cambios en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Hardware Changes (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos relacionados con cambios en el hardware de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con registros en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con registros en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Hardware Log (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos relacionados con registros en el hardware de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity1}**

- Supervisa eventos específicos de advertencias y errores de medios de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de medios de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de medios de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Media (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de medios de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con fallas previas en memorias de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con fallas previas en memorias de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSA en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSA en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSA en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell OMSA System (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos del sistema Dell OMSA en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSM en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSM en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos físicos Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos físicos Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos físicos Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).

- **zz[SYS] Hardware - Dell Physical Disk (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos relacionados con discos físicos Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con la administración de energía de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con la administración de energía de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores relacionados con la administración de energía de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Power Management (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de administración de energía de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 0 (Severity0).
- **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del procesador Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del procesador Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Processor (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos del procesador Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de máquinas espejo para redundancia de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de máquinas espejo para redundancia de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Redundancy Mirror (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de máquinas espejo para redundancia de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de temperatura de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de temperatura de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de temperatura de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Temperature (EWISFCV) - SYS - {Severity0}**

  - Supervisa eventos específicos de temperatura de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos virtuales Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos virtuales Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Virtual Disk (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos relacionados con discos virtuales Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - HP Top Tools (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de HP Top Tools en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - HP/Compaq Insight Manager (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de HP/Compaq Insight Manager en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - HP/Compaq StorageWorks (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de HP/Compaq StorageWorks en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - IBM SeriesX Events (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de eventos de IBM SeriesX en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de hardware diversos en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity2}**
  - Supervisa eventos específicos de errores de hardware diversos en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Misc HW (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias de hardware diversas en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

Infraestructura de red

- **zz[SYS] Network Infrastructure - Active Directory (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Network Infrastructure - Active Directory Events (E) - APP - {Severity3}**

  - Supervisa eventos específicos de errores de eventos de Active Directory en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Network Infrastructure - Active Directory Events (W) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias de eventos de Active Directory en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Network Infrastructure - Active Directory Logon/Logoff/Lockout Activity (F) - SEC - {Severity3}**
  - Supervisa eventos específicos de auditoría de errores en la actividad de inicio de sesión, cierre de sesión y bloqueo de Active Directory en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores NTDS de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores NTDS de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Network Infrastructure - Active Directory NTDS (I) - SYS - {Severity0}**
  - Supervisa eventos específicos de información de NTDS de Active Directory en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Network Infrastructure - DHCP Server (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de servidores DHCP en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - DHCP Server (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias de servidores DHCP en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - DNS Server (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de servidores DNS en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - DNS Server (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias de servidores DNS en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - WINS Server (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de servidores WINS en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

Acceso remoto

- **zz[SYS] Remote Access - Citrix MetaFrame (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Citrix MetaFrame en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Remote Access - Citrix Server Events (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de eventos del servidor Citrix en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de eventos del servidor Terminal Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de eventos del servidor Terminal Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).

Sistemas web

- **zz[SYS] Web Systems - IIS 6 Events (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de IIS 6 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de eventos de IIS 7 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de eventos de IIS 7 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Web Systems - IIS Server (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores del servidor IIS en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Web Systems - IIS Server (W) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias del servidor IIS en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).

Plataformas de SO

- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity2}**
  - Supervisa eventos específicos de errores comunes de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores comunes de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server (Core) Events (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos comunes de Windows Server en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity1}**
  - Supervisa eventos específicos de auditoría de errores comunes de Windows Server en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity3}**
  - Supervisa eventos específicos de auditoría de errores comunes de Windows Server en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias comunes de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias comunes de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server (Core) Ignore Events - (EW) - APP-SYS - {Ignore}**
  - Omite los ajustes de supervisión de eventos específicos de errores y advertencias comunes de Windows Server en los registros de eventos de la aplicación y del sistema.
- **zz[SYS] OS - Windows Server (Core) Printer Spooler (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del administrador de trabajos de impresión de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity2}**

- Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).

- **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (I) - SYS - {Severity2}**
  - Supervisa eventos específicos de información del administrador de control de servicios de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server (Core) System Shutdown (W) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias relacionadas con el apagado del sistema de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores comunes de Windows Server 2008 en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores comunes de Windows Server 2008 en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server 2008 (Core) Events (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias comunes de Windows Server 2008 en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server 2008 Advanced (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de Windows Server 2008 (avanzado) en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity1}**

- Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (básico) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (básico) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (básico) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server 2008 Basic (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de Windows Server 2008 (básico) en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity1}**
  - Supervisa eventos específicos de auditoría de errores de Windows Server 2008 (básico) en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity2}**
  - Supervisa eventos específicos de auditoría de errores de Windows Server 2008 (básico) en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity3}**
  - Supervisa eventos específicos de auditoría de errores de Windows Server 2008 (básico) en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Workstation (Core) Events (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores comunes de estaciones de trabajo Windows en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

Capítulo 4

Catálogo de contenido completo

En los siguientes temas, se resume la lista completa del contenido estándar proporcionado junto con el VSA.

En este capítulo

Vistas

Estado del Agente

- **zz[SYS] Agent - Has Checked In**
  - Muestra todas las máquinas que se registraron, al menos, una vez (excluye Plantillas).
- **zz[SYS] Agent - Has Not Checked In**
  - Muestra todos los agentes que no se registraron (es decir, computadoras y plantillas para implementación de KDS).
- **zz[SYS] Agent - Offline**
  - Muestra todos los agentes desconectados por más de 1 minuto.
- **zz[SYS] Agent - Offline 30+ Days**
  - Muestra todos los agentes desconectados por más de 30 días.
- **zz[SYS] Agent - Offline 60+ Days**
  - Muestra todos los agentes desconectados por más de 60 días.
- **zz[SYS] Agent - Online**
  - Muestra todos los agentes conectados en el último minuto.
- **zz[SYS] Agent - Online in Last 30 Days**
  - Muestra todos los agentes conectados en los últimos 7 días.
- **zz[SYS] Agent - Rebooted 14+ Days Ago**
  - Muestra todos los agentes que NO reiniciaron en los últimos 14 días.
- **zz[SYS] Agent - Suspended**
  - Muestra todos los agentes suspendidos.
- **zz[SYS] Agent - User Logged On**
  - Muestra todas las máquinas con un usuario que inició sesión en ellas.

Pestaña de Seguridad

- **zz[SYS] AV - AVG Technologies**
  - Muestra todas las máquinas que tienen el antivirus Grisoft AVG instalado.
- **zz[SYS] AV - Kaspersky ES**
  - Muestra todas las máquinas que tienen Kaspersky Endpoint Security instalado.
- **zz[SYS] AV - McAfee**
  - Muestra todas las máquinas que tienen el antivirus McAfee instalado.
- **zz[SYS] AV - Microsoft SE-FEP**
  - Muestra todas las máquinas que tienen Microsoft Security Essentials o Forefront Endpoint Protection instalados.
- **zz[SYS] AV - Sophos**
  - Muestra todas las máquinas que tienen el antivirus Sophos instalado.
- **zz[SYS] AV - Symantec AV**
  - Muestra todas las máquinas que tienen el antivirus Symantec instalado.
- **zz[SYS] AV - Symantec EP**
  - Muestra todas las máquinas que tienen el antivirus Symantec Endpoint Protection instalado.
- **zz[SYS] AV - Trend Micro**
  - Muestra todas las máquinas que tienen el antivirus Trend Micro instalado.

Respaldo

- **zz[SYS] Backup - CA BrightStor ARCServe**
  - Muestra todas las máquinas que tienen CA BrightStor ARCserve instalado.
- **zz[SYS] Backup - Symantec Backup Exec**
  - Muestra todas las máquinas que tienen Symantec Backup Exec instalado.

Hardware

- **zz[SYS] HW - Apple**
  - Muestra todas las máquinas cuyo fabricante sea Apple.
- **zz[SYS] HW - Dell**
  - Muestra todas las máquinas cuyo fabricante sea Dell.
- **zz[SYS] HW - Dell PowerEdge**
  - Muestra todas las máquinas cuyo fabricante sea Dell y cuyo nombre de producto sea PowerEdge.
- **zz[SYS] HW - HP**
  - Muestra todas las máquinas cuyo fabricante sea HP o Hewlett Packard.
- **zz[SYS] HW - HP ProLiant**
  - Muestra todas las máquinas cuyo fabricante sea HP o Hewlett Packard y cuyo nombre de producto sea ProLiant.
- **zz[SYS] HW - IBM**
  - Muestra todas las máquinas cuyo fabricante sea IBM.
- **zz[SYS] HW - IBM Series X**
  - Muestra todas las máquinas cuyo fabricante sea IBM y cuyo nombre de producto sea Series X.
- **zz[SYS] HW - Lenovo**
  - Muestra todas las máquinas cuyo fabricante sea Lenovo.
- **zz[SYS] HW - Not Portable**
  - Muestra todas las máquinas que no son móviles.
- **zz[SYS] HW - Portable**
  - Muestra todas las máquinas que son móviles (es decir, aquellas cuyo tipo de chasis sea un equipo portátil ligero, un equipo portátil regular, una Tablet PC, una computadora de bolsillo, una computadora miniportátil o una computadora ultraportátil). Nota: No incluyen máquinas con Mac OS X y Linux.
- **zz[SYS] HW - Under 1GB Memory**
  - Muestra todas las máquinas que tienen menos de 1 GB de memoria.
- **zz[SYS] HW - Under 512MB Memory**
  - Muestra todas las máquinas que tienen menos de 512 MB de memoria.
- **zz[SYS] HW - Virtual Guest**
  - Muestra todas las máquinas que son computadoras virtualizadas (invitados Hyper-V, VMWare, XenServer o VirtualBox).

Red

- **zz[SYS] Network - 10.11.12.x**
  - Muestra todos los agentes de la subred de red específica 10.11.12.x.

Sistema Operativo

- **zz[SYS] OS - All Linux**

- Muestra todos los equipos Linux.

- **zz[SYS] OS - All Mac OS X**
  - Muestra todas las máquinas Mac OS X.
- **zz[SYS] OS - All Mac OS X Servers**
  - Muestra todas las máquinas con plataformas Mac OS X Server.
- **zz[SYS] OS - All Mac OS X Workstations**
  - Muestra todas las máquinas con plataformas Mac OS X Workstation.
- **zz[SYS] OS - All Servers**
  - Muestra todas las máquinas en las que se ejecuta un sistema operativo tipo servidor.
- **zz[SYS] OS - All Windows**
  - Muestra todas las máquinas Windows.
- **zz[SYS] OS - All Windows SBS**
  - Muestra todas las máquinas en las que se ejecuta el servidor Windows SBS.
- **zz[SYS] OS - All Windows Servers**
  - Muestra todas las máquinas con Windows Server.
- **zz[SYS] OS - All Windows Workstations**
  - Muestra todas las estaciones de trabajo Windows.
- **zz[SYS] OS - All Workstations**
  - Muestra todas las máquinas en las que se ejecuta un sistema operativo tipo estación de trabajo.
- **zz[SYS] OS - Mac OS X 10.5 Leopard**
  - Muestra todas las máquinas con Mac OS X v10.5.
- **zz[SYS] OS - Mac OS X 10.6 Snow Leopard**
  - Muestra todas las máquinas con Mac OS X v10.6.
- **zz[SYS] OS - Mac OS X 10.7 Lion**
  - Muestra todas las máquinas con Mac OS X v10.7.
- **zz[SYS] OS - Mac OS X 10.8 Mountain Lion**
  - Muestra todas las máquinas con Mac OS X v10.8.
- **zz[SYS] OS - Win 2003 SBS**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Small Business Server de Windows 2003.
- **zz[SYS] OS - Win 2003 Server**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows Server 2003.
- **zz[SYS] OS - Win 2008 R2 Server**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Small Business Server de Windows 2008.
- **zz[SYS] OS - Win 2008 SBS**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows Server 2008.
- **zz[SYS] OS - Win 2008 Server**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows 2008 Server R2.
- **zz[SYS] OS - Win 2012 Server**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows Server 2012.

- **zz[SYS] OS - Win 7**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows 7.
- **zz[SYS] OS - Win Vista**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows Vista.
- **zz[SYS] OS - Win XP**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows XP.
- **zz[SYS] OS - Win 8**
  - Muestra todas las máquinas en las que se ejecuta el sistema operativo Windows 8.

Administración de Parche

- **zz[SYS] Patch - Deny Patching Policy**
  - Muestra todas las máquinas que forman parte de la directiva de parches “Deny Patching”.
- **zz[SYS] Patch - Missing 10+ Approved Patches**
  - Muestra todas las máquinas a las que les faltan 10 o más parches aprobados de acuerdo con su pertenencia a directivas de parches.
- **zz[SYS] Patch - Missing 20+ Approved Patches**
  - Muestra todas las máquinas a las que les faltan 20 o más parches aprobados de acuerdo con su pertenencia a directivas de parches.
- **zz[SYS] Patch - No Policy**
  - Muestra todas las máquinas que no pertenecen a ninguna directiva de parches.
- **zz[SYS] Patch - Pending Reboot**
  - Muestra todas las máquinas que tienen un reinicio pendiente, debido a las actualizaciones recientes de parches.
- **zz[SYS] Patch - Scan Failed**
  - Muestra todas las máquinas en las que se produjo un error en la detección de parches.
- **zz[SYS] Patch - Scan Not Scheduled**
  - Muestra todas las máquinas que no tienen programada una detección de parches.
- **zz[SYS] Patch - Server Patching Policy**
  - Muestra todas las máquinas que forman parte de la directiva de parches “Server Patching”.
- **zz[SYS] Patch - Servers w No Policy**
  - Muestra todas las máquinas que no pertenecen a ninguna directiva de parches.
- **zz[SYS] Patch - Test Patching Group**
  - Muestra todas las máquinas designadas como sistemas de prueba para la administración de parches.
- **zz[SYS] Patch - Windows Auto Update Enabled**
  - Muestra todas las máquinas que tienen habilitada la Actualización automática de Windows.
- **zz[SYS] Patch - Workstation Patching Policy**
  - Muestra todas las máquinas que forman parte de la directiva de parches “Workstation Patching”.
- **zz[SYS] Patch - Workstations w No Policy**
  - Muestra todas las máquinas que no pertenecen a ninguna directiva de parches.

Rol del servidor

- **zz[SYS] Role - Backup Exec Server**
  - Muestra todos los servidores Backup Exec.
- **zz[SYS] Role - Blackberry Server**
  - Muestra todos los servidores Blackberry Enterprise.

- **zz[SYS] Role - Brightstor ARCserve Server**
  - Muestra todos los servidores BrightStor ARCserve.
- **zz[SYS] Role - Citrix Server**
  - Muestra todos los servidores Citrix.
- **zz[SYS] Role - DHCP Server**
  - Muestra todos los servidores DHCP de MS.
- **zz[SYS] Role - DNS Server**
  - Muestra todos los servidores DNS de MS.
- **zz[SYS] Role - Domain Controller**
  - Muestra todos los servidores de controlador de dominio de AD de MS.
- **zz[SYS] Role - Exchange 2003 Server**
  - Muestra todos los servidores MS Exchange 2003.
- **zz[SYS] Role - Exchange 2007 Server**
  - Muestra todos los servidores MS Exchange 2007.
- **zz[SYS] Role - Exchange 2010 Server**
  - Muestra todos los servidores MS Exchange 2010.
- **zz[SYS] Role - Exchange Server**
  - Muestra todos los servidores MS Exchange.
- **zz[SYS] Role - File Server**
  - Muestra todos los servidores de archivos de MS.
- **zz[SYS] Role - FTP Server**
  - Muestra todos los servidores FTP de MS.
- **zz[SYS] Role - IIS Server**
  - Muestra todos los servidores MS IIS.
- **zz[SYS] Role - IMAP4 Server**
  - Muestra todos los servidores MS Exchange IMAP4.
- **zz[SYS] Role - POP3 Server**
  - Muestra todos los servidores MS Exchange POP3.
- **zz[SYS] Role - Print Server**
  - Muestra todos los servidores de impresión de MS.
- **zz[SYS] Role - SharePoint Server**
  - Muestra todos los servidores SharePoint de MS.
- **zz[SYS] Role - SMTP Server**
  - Muestra todos los servidores SMTP de MS.
- **zz[SYS] Role - SQL Server**
  - Muestra todos los servidores MS SQL Server.
- **zz[SYS] Role - SQL Server 2005**
  - Muestra todos los servidores MS SQL Server 2005.
- **zz[SYS] Role - SQL Server 2008**
  - Muestra todos los servidores MS SQL Server 2008.
- **zz[SYS] Role - Terminal Server**
  - Muestra todos los servidores Terminal Server de MS en modo de aplicación.
- **zz[SYS] Role - WINS Server**
  - Muestra todos los servidores WINS de MS.

Políticas

[System].Core.Global Policies.Agent Settings

- **Agent (Core)**
  - *Vista de directiva:* zz[SYS] Policy - Agent_Has Checked In
  - *Descripción:* Agent (Core): Applies common agent settings for all managed machines. Se habilita el ícono de Agente, pero sólo la opción Actualizar está disponible. El Control de registro se establece en 30 segundos con las siguientes opciones habilitadas: “Advertir si varios agentes usan la misma cuenta” y “Advertir si un agente en la misma LAN que el KServer se conecta a través de la puerta de enlace”. El Historial de registros de los agentes para todos los registros se establece en 31 días.
- **Windows Agent**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows
  - *Descripción:* Windows Agent: aplica la configuración de agente específica de Windows. Establece el Directorio de trabajo de agente en c:\kworking.
- **Linux Agent**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Linux
  - *Descripción:* Linux Agent: aplica la configuración de agente específica de Linux. Establece el Directorio de trabajo de agente en /tmp/kworking.
- **Macintosh Agent**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Mac OS X
  - *Descripción:* Macintosh Agent: aplica la configuración de agente específica de estaciones de trabajo Macintosh. Establece el Directorio de trabajo de agente en /Library/Kaseya/kworking.

[System].Core.Global Policies.Remote Support

- **Server RC Notification Policy (Silent w Admin Note)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Servers
  - *Descripción:* Server RC Notification Policy (Silent w Admin Note): aplica la configuración de notificación de control remoto en todos los servidores. Establece la opción Tomar control silenciosamente como tipo de notificación de usuario y habilita la opción Requerir nota del administrador para iniciar el control remoto.
- **Workstation RC Notification Policy (Alert/Term w Admin Note)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Workstations
  - *Descripción:* Workstation RC Notification Policy (Alert/Term w Admin Note): aplica ajustes de notificación de control remoto a todas las estaciones de trabajo. Establece las opciones “Si el usuario inició sesión, mostrar alerta” y “Notificar al usuario cuando finaliza la sesión” como tipo de notificación de usuario, y habilita la opción Requerir nota del administrador para iniciar el control remoto.

[System].Core.Org Specific Policies.Agent Settings

- **Agent (Hidden)**
  - *Vista de directiva:* zz[SYS] Policy - Agent_Has Checked In
  - *Descripción:* Agent (Hidden): aplica la configuración de agentes comunes a todas las máquinas administradas. El ícono de agente está deshabilitado/oculto. El Control de registro se establece en 30 segundos con las siguientes opciones habilitadas: “Advertir si varios agentes usan la misma cuenta” y “Advertir si un agente en la misma LAN que el KServer se conecta a través de la puerta de enlace”. El Historial de registros de los agentes para todos los registros se establece en 31 días.

- **Agent (Server)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Servers
  - *Descripción:* Agent (Server): aplica la configuración de agentes comunes a todos los servidores administrados. El ícono de agente se habilita con Deshabilitar control remoto, Actualizar y Salir. El Control de registro se establece en 30 segundos con las siguientes opciones habilitadas: “Advertir si varios agentes usan la misma cuenta” y “Advertir si un agente en la misma LAN que el KServer se conecta a través de la puerta de enlace”. El Historial de registros de los agentes para todos los registros se establece en 93 días.
- **Agent (Workstation)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Workstations
  - *Descripción:* Agent (Workstation): aplica la configuración de agentes comunes a todas las estaciones de trabajo administradas. El ícono de agente se habilita con Contactar al servicio de asistencia, Deshabilitar control remoto y Actualizar. El Control de registro se establece en 30 segundos con las siguientes opciones habilitadas: “Advertir si varios agentes usan la misma cuenta” y “Advertir si un agente en la misma LAN que el KServer se conecta a través de la puerta de enlace”. El Historial de registros de los agentes para todos los registros se establece en 31 días.

[System].Core.Org Specific Policies.Remote Support

- **Server RC Notification Policy (Silent w/o Admin Note)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Servers
  - *Descripción:* Server RC Notification Policy (Silent w/o Admin Note): aplica la configuración de notificación de control remoto en todos los servidores. Establece la opción Tomar control silenciosamente como tipo de notificación de usuario y no requiere una nota del administrador para iniciar el control remoto.
- **Workstation RC Notification Policy (Alert/Term w/o Admin Note)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Workstations
  - *Descripción:* Workstation RC Notification Policy (Alert/Term w/o Admin Note): aplica ajustes de notificación de control remoto a todas las estaciones de trabajo. Establece las opciones “Si el usuario inició sesión, mostrar alerta” y “Notificar al usuario cuando finaliza la sesión” como tipo de notificación de usuario, y no requiere una nota del administrador para iniciar el control remoto.
- **Workstation RC Notification Policy (Silent w Admin Note)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Workstations
  - *Descripción:* Workstation RC Notification Policy (Silent w Admin Note): aplica la configuración de notificación de control remoto en todas las estaciones de trabajo. Establece la opción Tomar control silenciosamente como tipo de notificación de usuario, pero requiere una nota del administrador para iniciar el control remoto.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Baseline.Baseline Audit Schedule (Annually Daytime)

- **Baseline Audit Schedule (Annually Jan 1-7 6am-6pm/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Agent_Has Checked In
  - *Descripción:* Baseline Audit Schedule (Annually Jan 1-7 6am-6pm/Power Mgmt): aplica una auditoría de base anual programada para todas las máquinas implementadas y registradas. Comienza el 1 de enero y se extiende hasta el 7 de enero entre las 06:00 y las 18:00. La directiva usa la característica de administración de energía en el momento programado de la auditoría e intenta encender aquellas máquinas que estén apagadas antes de la auditoría. Esta directiva suele aplicarse en situaciones en las que se requieren auditorías anuales con fines de planeación o cumplimiento. También se usan para realizar comparaciones pertinentes entre auditorías de base y las últimas auditorías, a fin de llevar a

cabo tareas operativas. La directiva puede aplicarse de forma selectiva a diversas máquinas, grupos de máquinas u organizaciones enteras de máquinas.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Daytime)

- **Latest/SysInfo Audit Schedule (Daily M-F 6am-6pm/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Agent_Has Checked In
  - *Descripción:* Latest/SysInfo Audit Schedule (Daily M-F 6am-6pm/Power Mgmt): aplica últimas auditorías y auditorías de información del sistema programadas a todas las máquinas registradas para que se lleven a cabo diariamente (de lunes a viernes) entre las 06:00 y las 18:00. La directiva usa la característica de administración de energía en el momento programado de la auditoría e intenta encender aquellas máquinas que estén apagadas antes de la auditoría. En general, se usa en situaciones en las que los clientes necesitan ejecutar auditorías durante los días de semana en horario laborable, ya que las máquinas suelen estar apagadas durante la noche y los fines de semana. La directiva puede aplicarse de forma selectiva a diversas máquinas, grupos de máquinas u organizaciones enteras de máquinas.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Nighttime)

- **Latest/SysInfo Audit Schedule (Daily M-F 6pm-6am/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Agent_Has Checked In
  - *Descripción:* Latest/SysInfo Audit Schedule (Daily M-F 6pm-6am/Power Mgmt): aplica últimas auditorías y auditorías de información del sistema programadas a todas las máquinas registradas para que se lleven a cabo diariamente (de lunes a viernes) entre las 18:00 y las 06:00. La directiva usa la característica de administración de energía en el momento programado de la auditoría e intenta encender aquellas máquinas que estén apagadas antes de la auditoría. En general, se usa en situaciones en las que los clientes prefieren ejecutar auditorías durante la noche cuando los sistemas se utilizan menos que durante el horario laborable y cuando las máquinas permanecen encendidas durante la noche o están configuradas para Wake On LAN o la administración de energía de vPro de manera que puedan encenderse a la noche en caso de que estén apagadas. La directiva puede aplicarse de forma selectiva a diversas máquinas, grupos de máquinas u organizaciones enteras de máquinas.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Weekly.Latest/SysInfo Audit Schedule (Weekly Daytime)

- **Latest/SysInfo Audit Schedule (Weekly M-F 6am-6pm/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Agent_Has Checked In
  - *Descripción:* Latest/SysInfo Audit Schedule (Weekly M-F 6am-6pm/Power Mgmt): aplica últimas auditorías y auditorías de información del sistema programadas a todas las máquinas registradas para que se lleven a cabo semanalmente (de lunes a viernes) entre las 06:00 y las 18:00. La directiva usa la característica de administración de energía en el momento programado de la auditoría e intenta encender aquellas máquinas que estén apagadas antes de la auditoría. En general, se usa en situaciones en las que los clientes necesitan ejecutar auditorías durante los días de semana en horario laborable, ya que las máquinas suelen estar apagadas durante la noche y los fines de semana. La directiva puede aplicarse de forma selectiva a diversas máquinas, grupos de máquinas u organizaciones enteras de máquinas.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Weekly.Latest/SysInfo Audit Schedule (Weekly Nighttime)

- **Latest/SysInfo Audit Schedule (Weekly M-F 6pm-6am/Power Mgmt)**

- *Vista de directiva:* zz[SYS] Policy - Agent_Has Checked In
- *Descripción:* Latest/SysInfo Audit Schedule (Weekly M-F 6pm-6am/Power Mgmt): aplica últimas auditorías y auditorías de información del sistema programadas a todas las máquinas registradas para que se lleven a cabo semanalmente (de lunes a viernes) entre las 18:00 y las 06:00. La directiva usa la característica de administración de energía en el momento programado de la auditoría e intenta encender aquellas máquinas que estén apagadas antes de la auditoría. En general, se usa en situaciones en las que los clientes prefieren ejecutar auditorías durante la noche cuando los sistemas se utilizan menos que durante el horario laborable y cuando las máquinas permanecen encendidas durante la noche o están configuradas para Wake On LAN o la administración de energía de vPro de manera que puedan encenderse a la noche en caso de que estén apagadas. La directiva puede aplicarse de forma selectiva a diversas máquinas, grupos de máquinas u organizaciones enteras de máquinas.

[System].Core.Org Specific Policies.Maintenance.Windows Workstation Recurring Maintenance

- **Windows Workstation Maintenance (Weekly M-F 6pm-6am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Workstations
  - *Descripción:* Windows Workstation Maintenance (Weekly M-F 6pm-6am): aplica un procedimiento programado de mantenimiento de las estaciones de trabajo Windows que se ejecuta semanalmente en todas las estaciones de trabajo Windows, de lunes a viernes, entre las 18:00 y las 06:00. Si la máquina no está encendida en el momento en el cual está programado el mantenimiento, la máquina omitirá ese ciclo de mantenimiento e intentará ejecutarlo de nuevo una semana después.

[System].Core.Org Specific Policies.Maintenance.Macintosh Workstation Recurring Maintenance

- **Macintosh Maintenance Schedule (Weekly M-F 6pm-6am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descripción:* Macintosh Maintenance Schedule (Weekly M-F 6pm-6am): aplica un procedimiento programado de mantenimiento de Macintosh que se ejecuta semanalmente en todas las máquinas Macintosh, de lunes a viernes, entre las 18:00 y las 06:00. Si la máquina no está encendida en el momento en el cual está programado el mantenimiento, la máquina omitirá ese ciclo de mantenimiento e intentará ejecutarlo de nuevo una semana después.

[System].Core.Org Specific Policies.Maintenance.Linux Recurring Maintenance

- **Linux Maintenance Schedule (Weekly M-F 6pm-6am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Linux
  - *Descripción:* Linux Maintenance Schedule (Weekly M-F 6pm-6am): aplica un procedimiento programado de mantenimiento de Linux que se ejecuta semanalmente en todas las máquinas Linux, de lunes a viernes, entre las 18:00 y las 06:00. Si la máquina no está encendida en el momento en el cual está programado el mantenimiento, la máquina omitirá ese ciclo de mantenimiento e intentará ejecutarlo de nuevo una semana después.

[System].Core.Org Specific Policies.Maintenance.Windows Server Recurring Maintenance

- **Windows Server Maintenance (Weekly Sun 12am-4am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Servers
  - *Descripción:* Windows Server Maintenance (Weekly Sun 12am-4am): aplica un procedimiento programado de mantenimiento de Windows Server que se ejecuta semanalmente en todas las máquinas con Windows Server, los domingos, entre las 00:00 y las 04:00. Si la máquina no está encendida en el momento en el cual está programado el mantenimiento, la máquina omitirá ese ciclo de mantenimiento e intentará ejecutarlo de nuevo una semana después.

[System].Core.Org Specific Policies.Monitoring.Server

- **Server Roles Enhanced Audit**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Servers
  - *Descripción:* Server Roles Enhanced Audit: aplica una auditoría mejorada programada que se ejecuta semanalmente, los domingos entre las 00:00 y las 04:00, a fin de identificar los roles funcionales del servidor para que se puedan aplicar las directivas de supervisión de manera adecuada de acuerdo con esos roles.
- **Common Windows Server Monitoring**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Servers
  - *Descripción:* Common Windows Server Monitoring: aplica un conjunto común de tareas de supervisión a todos los servidores Windows Server. Esto incluye la supervisión de los registros de eventos relacionados con el hardware, el Servicio de Windows y el rendimiento común de Windows.
- **Windows Server (Core)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Servers
  - *Descripción:* Windows Server (Core): aplica un conjunto de ajustes de supervisión de servicios básicos de Windows Server, en el que se incluyen la supervisión de servicios estándar, del rendimiento del sistema, de la elaboración de informes de estado y de los registros de eventos, entre otros.
- **Windows Server 2003**
  - *Vista de directiva:* zz[SYS] Policy - OS_Win 2003 Server
  - *Descripción:* Windows Server 2003: aplica ajustes de supervisión de servicio estándar para servidores Windows Server 2003.
- **Windows Server 2008/2008 R2**
  - *Vista de directiva:* zz[SYS] Policy - OS_Win 2008 Server
  - *Descripción:* Windows Server 2008/2008 R2: aplica ajustes de supervisión de servicio estándar para servidores Windows Server 2008/2008 R2.
- **Windows Server 2012**
  - *Vista de directiva:* zz[SYS] Policy - OS_Win 2012 Server
  - *Descripción:* Windows Server 2012: aplica ajustes de supervisión de servicio estándar para servidores Windows Server 2012.

[System].Core.Org Specific Policies.Monitoring.Server.Hardware

- **Dell PowerEdge**
  - *Vista de directiva:* zz[SYS] Policy - HW_Dell PowerEdge
  - *Descripción:* Dell PowerEdge: aplica ajustes de supervisión y alerta específicos del hardware de servidores Dell PowerEdge. Es posible que este tipo de supervisión requiera la instalación de herramientas de administración específicas de los servidores Dell PowerEdge en la máquina servidor.
- **HP ProLiant**
  - *Vista de directiva:* zz[SYS] Policy - HW_HP ProLiant
  - *Descripción:* HP ProLiant: aplica ajustes de supervisión y alerta específicos del hardware de servidores HP ProLiant. Es posible que este tipo de supervisión requiera la instalación de herramientas de administración específicas de los servidores HP ProLiant en la máquina servidor.
- **IBM Series x**
  - *Vista de directiva:* zz[SYS] Policy - HW_IBM Series X
  - *Descripción:* IBM Series x: aplica ajustes de supervisión y alerta específicos del hardware de servidores IBM Series X. Es posible que este tipo de supervisión requiera la

instalación de herramientas de administración específicas de los servidores IBM Series X en la máquina servidor.

[System].Core.Org Specific Policies.Monitoring.Server.Roles

- **Backup Exec Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Backup Exec Server
  - *Descripción:* Backup Exec Server: aplica ajustes de supervisión a servidores Backup Exec.
- **Servidor Blackberry Enterprise**
  - *Vista de directiva:* zz[SYS] Policy - Role_Blackberry Server
  - *Descripción:* Blackberry Enterprise Server: aplica ajustes de supervisión a servidores Blackberry Enterprise Server.
- **BrightStor ARCServe Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Brightstor ARCserve Server
  - *Descripción:* BrightStor ARCServe Server: aplica ajustes de supervisión a servidores BrightStor.
- **Citrix Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Citrix Server
  - *Descripción:* Citrix Server: aplica ajustes de supervisión a servidores Citrix.
- **Servidor DHCP**
  - *Vista de directiva:* zz[SYS] Policy - Role_DHCP Server
  - *Descripción:* DHCP Server: aplica ajustes de supervisión a servidores DHCP.
- **Servidor DNS**
  - *Vista de directiva:* zz[SYS] Policy - Role_DNS Server
  - *Descripción:* DNS Server: aplica ajustes de supervisión a servidores DNS.
- **Controlador de dominio**
  - *Vista de directiva:* zz[SYS] Policy - Role_Domain Controller
  - *Descripción:* Domain Controller: aplica ajustes de supervisión a los controladores de dominio.
- **Exchange 2003 Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Exchange 2003 Server
  - *Descripción:* Exchange 2003 Server: aplica ajustes de supervisión a servidores Exchange 2003.
- **Exchange 2007 Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Exchange 2007 Server
  - *Descripción:* Exchange 2007 Server: aplica ajustes de supervisión a servidores Exchange 2007.
- **Exchange 2010 Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Exchange 2010 Server
  - *Descripción:* Exchange 2010 Server: aplica ajustes de supervisión a servidores Exchange 2010.
- **Exchange Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Exchange Server
  - *Descripción:* Exchange Server: aplica ajustes de supervisión a servidores Exchange.
- **Servidor de Archivo**
  - *Vista de directiva:* zz[SYS] Policy - Role_File Server
  - *Descripción:* File Server: aplica ajustes de supervisión a servidores de archivos.

- **FTP Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_FTP Server
  - *Descripción:* FTP Server: aplica ajustes de supervisión a servidores FTP.
- **IIS Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_IIS Server
  - *Descripción:* IIS Server: aplica ajustes de supervisión a servidores IIS.
- **IMAP4 Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_IMAP4 Server
  - *Descripción:* IMAP4 Server: aplica ajustes de supervisión a servidores IMAP4.
- **POP3 Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_POP3 Server
  - *Descripción:* POP3 Server: aplica ajustes de supervisión a servidores POP3.
- **Print Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Print Server
  - *Descripción:* Print Server: aplica ajustes de supervisión a servidores de impresión.
- **SharePoint Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_SharePoint Server
  - *Descripción:* SharePoint Server: aplica ajustes de supervisión a servidores SharePoint.
- **SMTP Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_SMTP Server
  - *Descripción:* SMTP Server: aplica ajustes de supervisión a servidores SMTP.
- **Servidor SQL**
  - *Vista de directiva:* zz[SYS] Policy - Role_SQL Server
  - *Descripción:* SQL Server: aplica ajustes de supervisión a servidores SQL Server.
- **SQL Server 2005**
  - *Vista de directiva:* zz[SYS] Policy - Role_SQL Server 2005
  - *Descripción:* SQL Server 2005: aplica ajustes de supervisión a servidores SQL Server 2005.
- **SQL Server 2008**
  - *Vista de directiva:* zz[SYS] Policy - Role_SQL Server 2008
  - *Descripción:* SQL Server 2008: aplica ajustes de supervisión a servidores SQL Server 2008.
- **Terminal Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_Terminal Server
  - *Descripción:* Terminal Server: aplica ajustes de supervisión a servidores Terminal Server.
- **WINS Server**
  - *Vista de directiva:* zz[SYS] Policy - Role_WINS Server
  - *Descripción:* WINS Server: aplica ajustes de supervisión a servidores WINS.

[System].Core.Org Specific Policies.Monitoring.Workstation

- **Common Windows Workstation Monitoring**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Workstations
  - *Descripción:* Common Windows Workstation Monitoring: aplica un conjunto común de ajustes de supervisión a todas las estaciones de trabajo Windows. Esto incluye la

supervisión de los registros de eventos relacionados con el hardware, el Servicio de Windows y el rendimiento común de Windows.

- **Windows Workstation (Core)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Workstations
  - *Descripción:* Windows Workstation (Core): aplica un conjunto de ajustes de supervisión de servicios básicos de estaciones de trabajo Windows, en el que se incluyen la supervisión de servicios estándar, del rendimiento del sistema y de la elaboración de informes de estado, entre otros.
- **Windows Vista**
  - *Vista de directiva:* zz[SYS] Policy - OS_Win Vista
  - *Descripción:* Windows Vista: aplica ajustes de supervisión de servicio estándar para máquinas con Windows Vista.
- **Windows 7**
  - *Vista de directiva:* zz[SYS] Policy - OS_Win 7
  - *Descripción:* Windows 7: aplica ajustes de supervisión de servicio estándar para máquinas con Windows 7.
- **Windows XP**
  - *Vista de directiva:* zz[SYS] Policy - OS_Win XP
  - *Descripción:* Windows XP: aplica ajustes de supervisión de servicio estándar para máquinas con Windows XP.
- **Windows 8**
  - *Vista de directiva:* zz[SYS] Policy - OS_Win 8
  - *Descripción:* Windows 8: aplica ajustes de supervisión de servicio estándar para máquinas con Windows 8.

[System].Core.Org Specific Policies.Monitoring.Security.Anti-Virus

- **AVG Tech**
  - *Vista de directiva:* zz[SYS] Policy - AV_AVG Technologies
  - *Descripción:* McAfee: aplica ajustes de supervisión para los antivirus AVG Technologies.
- **Kaspersky ES**
  - *Vista de directiva:* zz[SYS] Policy - AV_Kaspersky ES
  - *Descripción:* Kaspersky ES: aplica ajustes de supervisión para Kaspersky Endpoint Security.
- **McAfee**
  - *Vista de directiva:* zz[SYS] Policy - AV_McAfee
  - *Descripción:* McAfee: aplica ajustes de supervisión para los antivirus McAfee.
- **Microsoft SE-FEP**
  - *Vista de directiva:* zz[SYS] Policy - AV_Microsoft SE-FEP
  - *Descripción:* Microsoft SE-FEP: aplica ajustes de supervisión para Microsoft Security Essentials y Forefront Endpoint Protection.
- **Sophos**
  - *Vista de directiva:* zz[SYS] Policy - AV_Sophos
  - *Descripción:* Sophos: aplica ajustes de supervisión para los antivirus Sophos.
- **Symantec AV**
  - *Vista de directiva:* zz[SYS] Policy - AV_Symantec AV
  - *Descripción:* Symantec zz[SYS] AV: aplica ajustes de supervisión para los antivirus Symantec.

- **Symantec EP**
  - *Vista de directiva:* zz[SYS] Policy - AV_Symantec EP
  - *Descripción:* Symantec EP: aplica ajustes de supervisión para Symantec Endpoint Protection.
- **Trend Micro**
  - *Vista de directiva:* zz[SYS] Policy - AV_Trend Micro
  - *Descripción:* Trend Micro: aplica ajustes de supervisión para los antivirus Trend Micro.

[System].Core.Org Specific Policies.Monitoring.Utility

- **Actualizar Listas por Exploración**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows
  - *Descripción:* Update Lists By Scan: programa una actualización de listas mediante análisis para que se ejecute en todas las máquinas Windows para mantener actualizada la información sobre el contador de rendimiento, el registro de eventos y los servicios en ejecución de cada máquina, a fin de lograr una supervisión precisa.
- **Monitoring Cleanup**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows
  - *Descripción:* Monitoring Cleanup: como última directiva con conjuntos de alertas y monitores, esta directiva garantiza de manera efectiva la eliminación de los ajustes de supervisión aplicados anteriormente (alertas de registros de eventos y conjuntos de monitores asignados por medio de otras directivas que ya no son necesarias debido a cambios de rol, etc.).

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Common Windows Patch Mgmt Settings

- **Deny Patch Settings**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Deny Patching Group
  - *Descripción:* Deny Patch Settings: aplica ajustes de administración de parches a las máquinas seleccionadas en la vista 'zz[SYS] Policy - Deny Patching Group'. Establece la Acción de reinicio en “Si el usuario inició sesión, solicitarle que reinicie cada 60 minutos hasta que se produzca el reinicio. Reiniciar si el usuario no inició sesión”. Establece la pertenencia a la directiva de parches en la directiva de parches “Deny Patching”. Establece las alertas de parches de manera que se genere una alarma y se envíe un correo electrónico a la dirección de alertas de parches cuando se produce un error en la instalación de un parche o cuando la credencial de agente no es válida o falta.
- **Test Patch Settings**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Test Patching Group
  - *Descripción:* Test Patch Settings: aplica ajustes de administración de parches a las máquinas seleccionadas en la vista 'zz[SYS] Policy - Test Patching Group'. Establece la Acción de reinicio en “Si el usuario inició sesión, solicitarle que reinicie cada 60 minutos hasta que se produzca el reinicio. Reiniciar si el usuario no inició sesión”. Establece la pertenencia a la directiva de parches en la directiva de parches “Test Patching”. Establece las alertas de parches de manera que se genere una alarma y se envíe un correo electrónico a la dirección de alertas de parches cuando se produce un error en la instalación de un parche o cuando la credencial de agente no es válida o falta.
- **Deshabilitar Actualización Automática de Windows**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Windows Auto Update Enabled
  - *Descripción:* Deshabilita las actualizaciones automáticas de Windows en las máquinas que las tienen habilitadas. Si la actualización automática de Windows está habilitada y la administración de parches de Kaseya está en uso, dicha actualización puede entrar en

conflicto con la estrategia de administración de parches de Kaseya, y esto puede derivar en la implementación de parches denegados o que aún no fueron aprobados por Kaseya.

- **File Source Internet**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows
  - *Descripción:* File Source Internet: establece el Origen de archivo para la administración de parches en Internet para todos los equipos Windows de manera que los parches se descarguen directamente de los servidores de descarga y parches de Microsoft. Esta es la directiva predeterminada, y puede ser sustituida por una directiva alternativa que se aplique a determinadas organizaciones o grupos de máquinas y que tenga precedencia sobre esta directiva.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Workstation Patch Mgmt Settings

- **Workstation Patch Settings**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Workstations
  - *Descripción:* Workstation Patch Settings: aplica ajustes de administración de parches a las estaciones de trabajo Windows. Establece la Acción de reinicio en “Si el usuario inició sesión, solicitarle que reinicie cada 60 minutos hasta que se produzca el reinicio. Reiniciar si el usuario no inició sesión”. Establece la pertenencia a la directiva de parches en la directiva de parches “Workstation Patching”. Establece las alertas de parches de manera que se genere una alarma y se envíe un correo electrónico a la dirección de alertas de parches cuando se produce un error en la instalación de un parche o cuando la credencial de agente no es válida o falta.
- **Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6am-6pm/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Descripción:* Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6am-6pm/Power Mgmt): aplica programaciones de actualizaciones automáticas diarias a los miembros de la directiva Workstation Patching a los que les falten 10 o más parches aprobados. Las actualizaciones automáticas se programan para llevarse a cabo de lunes a viernes, todas las semanas, entre las 06:00 y las 18:00. Esta directiva suele utilizarse cuando los clientes tienen máquinas a las que les faltan algunos pocos parches y desean actualizar esos sistemas en el transcurso de algunos días, en lugar de tener que esperar semanas o meses. Una vez que se instalan parches en las máquinas, ya no es necesario volver a hacerlo a diario. Las actualizaciones automáticas se llevan a cabo durante el día en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.
- **Weekly Wkst Schedule (Scan Tu 6am-6pm/Auto Update W 6am-6pm/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Descripción:* Weekly Wkst Schedule (Scan Tu 6am-6pm/Auto Update W 6am-6pm/Power Mgmt): aplica programaciones semanales de detección de parches y actualizaciones automáticas a los miembros de la directiva Workstation Patching. Las detecciones de parches se programan para llevarse a cabo los martes de cada semana de 06:00 a 18:00 y las actualizaciones automáticas, los miércoles de cada semana en la misma franja horaria. Esta directiva suele utilizarse cuando los clientes desean adoptar un enfoque más agresivo en lo que respecta a la aplicación parches, a fin de minimizar los riesgos derivados de la falta de estos en las máquinas, y, por ese motivo, quieren que los parches nuevos se instalen relativamente rápido en las máquinas. Las actualizaciones automáticas se llevan a cabo durante el día en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Server Patch Mgmt Settings

- **Server Patch Settings**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Servers
  - *Descripción:* Server Patch Settings: aplica ajustes de administración de parches a los servidores Windows. Establece la Acción de reinicio en “No reiniciar después de la actualización”, “Cuando se requiera reiniciar, enviar correo electrónico a la dirección de alertas de parches”. Establece la pertenencia a la directiva de parches en la directiva de parches “Server Patching”. Establece las alertas de parches de manera que se genere una alarma y se envíe un correo electrónico a la dirección de alertas de parches cuando se produce un error en la instalación de un parche o cuando la credencial de agente no es válida o falta.
- **Weekly Srvr Schedule (Scan W 6pm-6am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Windows Servers
  - *Descripción:* Weekly Srvr Schedule (Scan W 6pm-6am): aplica una programación de detección de parches a los miembros de la directiva de parches de servidores. Las detecciones de parches se programan para llevarse a cabo los miércoles de cada semana de 18:00 a 06:00. Según esta directiva, no se programan implementaciones de actualizaciones automáticas de parches.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Other Windows Patch Mgmt Settings

- **File Source System Server**
  - *Vista de directiva:* zz[SYS] Policy - Network_10.11.12.x
  - *Descripción:* File Source System Server: establece el Origen de archivo para la administración de parches en el servidor del sistema para todos los equipos Windows de manera que este servidor descargue los parches de manera centralizada y que luego, desde allí, estos se distribuyan hacia las máquinas a las cuales se les aplicarán los parches.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Other Windows Patch Mgmt Settings.Other Schedules.Daytime

- **Monthly Wkst Schedule (Scan 2nd W 6am-6pm/Auto Update 1st W 6am-6pm/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Descripción:* Monthly Wkst Schedule (Scan 2nd W 6am-6pm/Auto Update 1st W 6am-6pm/Power Mgmt): aplica programaciones mensuales de detección de parches y actualizaciones automáticas a los miembros de la directiva de aplicación de parches de estaciones de trabajo. Las detecciones de parches se programan para llevarse a cabo el segundo miércoles de cada mes de 06:00 a 18:00. Las actualizaciones automáticas se programan para llevarse a cabo el primer miércoles de cada mes de 06:00 a 18:00. Esta directiva suele utilizarse cuando los clientes desean adoptar un enfoque más conservador en lo que respecta a la administración de parches, ya que los análisis y las actualizaciones se llevan a cabo una vez al mes y las actualizaciones se implementan a principio de mes. Esto significa que el lanzamiento de los parches implementados se realizó al menos un mes atrás, lo cual permite evaluar los parches de manera exhaustiva antes de su implementación general. Los análisis y las actualizaciones automáticas se llevan a cabo durante el día en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Workstation Patch Mgmt Settings.Nighttime

- **Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6pm-6am/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Descripción:* Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6pm-6am/Power Mgmt): aplica programaciones de actualizaciones automáticas diarias a los miembros de la directiva Workstation Patching a los que les falten 10 o más parches aprobados. Las actualizaciones automáticas se programan para llevarse a cabo de lunes a viernes, todas las semanas, entre las 18:00 y las 06:00. Esta directiva suele utilizarse cuando los clientes tienen máquinas a las que les faltan algunos pocos parches y desean actualizar esos sistemas en el transcurso de algunos días, en lugar de tener que esperar semanas o meses. Una vez que se instalan parches en las máquinas, ya no es necesario volver a hacerlo a diario. Las actualizaciones automáticas se llevan a cabo durante la noche para mitigar la interrupción del servicio; asimismo, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen puedan encenderse antes de estas operaciones.
- **Weekly Wkst Schedule for 10+ Patches (Auto Update W 6pm-6am/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Descripción:* Weekly Wkst Schedule for 10+ Patches (Auto Update W 6pm-6am/Power Mgmt): aplica programaciones de actualizaciones automáticas diarias a los miembros de la directiva Workstation Patching a los que les falten 10 o más parches aprobados. Las actualizaciones automáticas se programan para llevarse a cabo los miércoles de cada semana de 18:00 a 06:00. Esta directiva suele utilizarse cuando los clientes tienen máquinas a las que les faltan algunos pocos parches y desean actualizar esos sistemas en el transcurso de algunas semanas, en lugar de tener que esperar meses. Una vez que los parches se aplican a las máquinas, ya no deberán aplicarse en forma semanal, y los equipos recurrirán a una programación mensual de detección de parches y de actualización automática. Las actualizaciones automáticas se llevan a cabo durante la noche en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.
- **Weekly Wkst Schedule (Scan Tu 6pm-6am/Auto Update W 6pm-6am/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Descripción:* Weekly Wkst Schedule (Scan Tu 6pm-6am/Auto Update W 6pm-6am/Power Mgmt): aplica programaciones semanales de detección de parches y actualizaciones automáticas a los miembros de la directiva Workstation Patching. Las detecciones de parches se programan para llevarse a cabo los martes de cada semana de 18:00 a 06:00 y las actualizaciones automáticas, los miércoles de cada semana en la misma franja horaria. Esta directiva suele utilizarse cuando los clientes desean adoptar un enfoque más agresivo en lo que respecta a la aplicación parches, a fin de minimizar los riesgos derivados de la falta de estos en las máquinas, y, por ese motivo, quieren que los parches nuevos se instalen relativamente rápido en las máquinas. Los análisis y las actualizaciones automáticas se llevan a cabo durante la noche para mitigar la interrupción del servicio; asimismo, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen puedan encenderse antes de estas operaciones.
- **Monthly Wkst Schedule (Scan 2nd W 6pm-6am/Auto Update 1st W 6pm-6am/Power Mgmt)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Descripción:* Monthly Wkst Schedule (Scan 2nd W 6pm-6am/Auto Update 1st W 6pm-6am/Power Mgmt): aplica programaciones mensuales de detección de parches y actualizaciones automáticas a los miembros de la directiva de aplicación de parches de estaciones de trabajo. Los análisis de parches se programan para llevarse a cabo el

segundo miércoles de cada mes de 18:00 a 06:00. Las actualizaciones automáticas se programan para llevarse a cabo el primer miércoles de cada mes de 18:00 a 06:00. Los análisis y las actualizaciones automáticas se llevan a cabo durante la noche para mitigar la interrupción del servicio; asimismo, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen puedan encenderse antes de estas operaciones. Esta directiva suele utilizarse cuando los clientes desean adoptar un enfoque más conservador en lo que respecta a la administración de parches, ya que los análisis y las actualizaciones se llevan a cabo una vez al mes y las actualizaciones se implementan a principio de mes. Esto significa que el lanzamiento de los parches implementados se realizó al menos un mes atrás, lo cual permite evaluar los parches de manera exhaustiva antes de su implementación general.

- **Monthly Srvr Schedule (Scan 2nd W 6pm-6am)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Server Patching Policy
  - *Descripción:* Monthly Srvr Schedule (Scan 2nd W 6pm-6am): aplica una programación de detección de parches a los miembros de la directiva de parches de servidores. Los análisis de parches se programan para llevarse a cabo el segundo miércoles de cada mes de 18:00 a 06:00. Según esta directiva, no se programan implementaciones de actualizaciones automáticas de parches.
- **Monthly Srvr Schedule (Scan 2nd W 6pm-6am/Auto Update 1st Su 12am-4am)**
  - *Vista de directiva:* zz[SYS] Policy - Patch_Server Patching Policy
  - *Descripción:* Monthly Srvr Schedule (Scan 2nd W 6pm-6am/Auto Update 1st Su 12am-4am): aplica programaciones mensuales de detección de parches y actualizaciones automáticas a los miembros de la directiva de aplicación de parches de servidores. Las detecciones de parches se programan para llevarse a cabo el segundo miércoles de cada mes de 06:00 a 18:00. Las actualizaciones automáticas se programan para llevarse a cabo el primer domingo de cada mes de 00:00 a 04:00. Esta directiva suele utilizarse cuando los clientes desean adoptar un enfoque más conservador en lo que respecta a la administración de parches, ya que los análisis y las actualizaciones se llevan a cabo una vez al mes y las actualizaciones se implementan a principio de mes. Esto significa que el lanzamiento de los parches implementados se realizó al menos un mes atrás, lo cual permite evaluar los parches de manera exhaustiva antes de su implementación general. Los análisis y las actualizaciones automáticas se llevan a cabo durante el fin de semana, temprano por la mañana, a fin de reducir el impacto en el tiempo de producción y los usuarios que podría tener una interrupción del servicio relacionada con los servidores en los que se aplican los parches.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Workstation Software Update Settings

- **Weekly Macintosh Workstation Software Update (Install Recommended W 6am-6pm)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descripción:* Weekly Macintosh Workstation Software Update (Install Recommended W 6am-6pm): aplica una actualización de software Mac para que se ejecute los miércoles de cada semana de 06:00 a 18:00 y por medio de la cual se instalan las actualizaciones de software Macintosh recomendadas en las estaciones de trabajo Macintosh. Las actualizaciones de software se llevan a cabo durante el día en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Server Software Update Settings

- **Monthly Macintosh Server Software Update (Install Recommended 1st Su 12am-4am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Mac OS X Servers

- *Descripción:* Monthly Macintosh Server Software Update (Install Recommended 1st Su 12am-4am): aplica una actualización de software Mac para que se ejecute el primer domingo de cada mes y por medio de la cual se instalan las actualizaciones de software Macintosh recomendadas en los servidores Macintosh. Gracias a esto, los servidores Mac se mantendrán al día con las actualizaciones recomendadas.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Other Macintosh Software Update Settings

- **Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6am-6pm)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descripción:* Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6am-6pm): aplica una actualización de software Mac para que se ejecute el primer miércoles de cada mes y por medio de la cual se instalan las actualizaciones de software Macintosh recomendadas en las estaciones de trabajo Macintosh. Las actualizaciones de software se llevan a cabo durante el día en el caso de los clientes que suelen apagar las máquinas durante la noche. No obstante, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen durante el día puedan encenderse antes de estas operaciones.
- **Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6pm-6am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descripción:* Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6pm-6am): aplica una actualización de software Mac para que se ejecute el primer miércoles de cada mes de 18:00 a 06:00 y por medio de la cual se instalan las actualizaciones de software Macintosh recomendadas en las estaciones de trabajo Macintosh. Las actualizaciones de software se llevan a cabo durante la noche para mitigar la interrupción del servicio; asimismo, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen puedan encenderse antes de estas operaciones.
- **Monthly Macintosh Workstation Software Update (Install All 1st W 6pm-6am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descripción:* Monthly Macintosh Workstation Software Update (Install All 1st W 6pm-6am): aplica una actualización de software Mac para que se ejecute el primer miércoles de cada mes de 18:00 a 06:00 y por medio de la cual se instalan las actualizaciones de software Macintosh recomendadas en las estaciones de trabajo Macintosh. Las actualizaciones de software se llevan a cabo durante la noche para mitigar la interrupción del servicio; asimismo, la opción de administración de energía está habilitada en estas programaciones, a fin de que las máquinas que se apaguen puedan encenderse antes de estas operaciones.

[System].Core.Org Specific Policies.Patch / Update Management.Linux

- **Monthly Linux Package Updates/Upgrades (Install 1st W 6pm-6am)**
  - *Vista de directiva:* zz[SYS] Policy - OS_All Linux
  - *Descripción:* Monthly Linux Package Updates/Upgrades (Install 1st W 6pm-6am): aplica actualizaciones de paquetes Linux para que se ejecuten el primer miércoles de cada mes. Esto mantendrá actualizadas las máquinas Linux en lo que respecta a los distintos componentes de software instalados.

Detalles sobre directivas de parches

Deny Patching	Directiva de aprobación predeterminada
Actualización de Seguridad (Prioridad Alta)	Denegada
Actualización de Seguridad - Importante (Prioridad Alta)	Denegada
Actualización de Seguridad - Moderada (Prioridad Alta)	Denegada
Actualización de Seguridad - Baja (Prioridad Alta)	Denegada
Actualización de Seguridad - No Especificada (Prioridad Alta)	Denegada
Actualización Crítica (Prioridad Alta)	Denegada
Actualizar Rollup (Prioridad Alta)	Denegada
Service Pack (Opcional - Software)	Denegada
Actualización (Opcional - Software)	Denegada
Paquete de Función (Opcional - Software)	Denegada
Herramienta (Opcional - Software)	Denegada
Server Patching	
Actualización de Seguridad (Prioridad Alta)	Aprobación Pendiente
Actualización de Seguridad - Importante (Prioridad Alta)	Aprobación Pendiente
Actualización de Seguridad - Moderada (Prioridad Alta)	Aprobación Pendiente
Actualización de Seguridad - Baja (Prioridad Alta)	Aprobación Pendiente
Actualización de Seguridad - No Especificada (Prioridad Alta)	Aprobación Pendiente
Actualización Crítica (Prioridad Alta)	Aprobación Pendiente
Actualizar Rollup (Prioridad Alta)	Aprobación Pendiente
Service Pack (Opcional - Software)	Aprobación Pendiente
Actualización (Opcional - Software)	Aprobación Pendiente
Paquete de Función (Opcional - Software)	Aprobación Pendiente
Herramienta (Opcional - Software)	Aprobación Pendiente
Test Patching	
Actualización de Seguridad (Prioridad Alta)	Aprobada
Actualización de Seguridad - Importante (Prioridad Alta)	Aprobada
Actualización de Seguridad - Moderada (Prioridad Alta)	Aprobada
Actualización de Seguridad - Baja (Prioridad Alta)	Aprobada
Actualización de Seguridad - No Especificada (Prioridad Alta)	Aprobada
Actualización Crítica (Prioridad Alta)	Aprobada
Actualizar Rollup (Prioridad Alta)	Aprobación Pendiente
Service Pack (Opcional - Software)	Aprobación Pendiente
Actualización (Opcional - Software)	Aprobación Pendiente
Paquete de Función (Opcional - Software)	Aprobación Pendiente
Herramienta (Opcional - Software)	Aprobación Pendiente

Workstation Patching

Actualización de Seguridad (Prioridad Alta)	Aprobada
Actualización de Seguridad - Importante (Prioridad Alta)	Aprobada
Actualización de Seguridad - Moderada (Prioridad Alta)	Aprobada
Actualización de Seguridad - Baja (Prioridad Alta)	Aprobada
Actualización de Seguridad - No Especificada (Prioridad Alta)	Aprobada
Actualización Crítica (Prioridad Alta)	Aprobada
Actualizar Rollup (Prioridad Alta)	Aprobación Pendiente
Service Pack (Opcional - Software)	Aprobación Pendiente
Actualización (Opcional - Software)	Aprobación Pendiente
Paquete de Función (Opcional - Software)	Aprobación Pendiente
Herramienta (Opcional - Software)	Aprobación Pendiente

Procedimientos del Agente

En esta sección

Core.0 Common Procedures

Core.0 Common Procedures.Reboot/Shutdown/Logoff

- **Forzar Desconexión de Usuario**
  - Desconecta al usuario actualmente conectado.
- **Reiniciar-No-Preguntar**
  - Si el usuario se encuentra conectado, preguntarle si está bien reiniciar; asumir no luego de 5 min. Si el usuario no se encuentra conectado, continuar y reiniciar. Este script llama Reiniciar-No-Preguntar-2 para preguntar al usuario.
- **Reiniciar-No-Preguntar-2**
  - ***¡NO PROGRAMAR ESTE SCRIPT! *** Este script es invocado por el script Reboot-Ask-No y no debe programarse por sí solo.
- **Reiniciar-Preguntar-Sí**
  - Si el usuario se encuentra conectado, preguntarle si está bien reiniciar; asumir sí luego de 5 min. Si el usuario no se encuentra conectado, continuar y reiniciar. Este script llama Reiniciar-Sí-Preguntar-2 para preguntar al usuario.
- **Reiniciar-Preguntar-Sí-2**
  - ***¡NO PROGRAMAR ESTE SCRIPT! *** Este script es invocado por el script Reboot-Ask-Yes y no debe programarse por sí solo.
- **Reiniciar- Forzar**

- Fuerza un reinicio inmediato.

- **Reiniciar-Nag**
  - Si el usuario se encuentra conectado, preguntarle sobre el reinicio cada 5 minutos hasta que el usuario permita el reinicio. Si el usuario no se encuentra conectado, continuar y reiniciar. Este script llama Reiniciar-Nag-2 para preguntar al usuario.
- **Reiniciar-Nag-2**
  - ***¡NO PROGRAMAR ESTE SCRIPT! *** Este script es invocado por el script Reboot-Nag y no debe programarse por sí solo.
- **Reiniciar-Usuario-No**
  - Reinicia la máquina sólo si un usuario no se encuentra conectado.
- **Reiniciar-Advertir**
  - Si el usuario está conectado, advertir al usuario que se reiniciará la máquina en 5 min. Si el usuario no se encuentra conectado, continuar y reiniciar.
- **Reboot - Prompt User to reboot every 15 mins until they answer Yes**
  - Este script solicitará al usuario que reinicie cada 15 minutos.
- **Shutdown Computer**
  - Apaga la máquina con agente por medio de la utilidad shutdown.exe de Windows.

Core.1 Windows Procedures

Core.1 Windows Procedures.Desktops.Auditing

- **Audit BIOS Info via WMI**
  - Usa WMIC para obtener información del BIOS, la transcribe en un archivo, lo recupera y lo envía a la carpeta GetFile() del sistema. Luego escribe una entrada en el registro de procedimientos de agente con la información del BIOS detectada.
- **Audit BOOT.INI**
  - Audita el contenido de C:\BOOT.INI (si existe), escribe una entrada en el registro de procedimientos de agente, recupera una copia de BOOT.INI y la envía a la carpeta GetFile() del sistema.
- **Audit Files (Any File Types Entered)**
  - Busca todos los archivos por medio de un conjunto de máscaras de archivos que se introducen al programar el procedimiento y crea un archivo de registro TXT simple y un archivo CSV sobre la base de los nombres de archivos que se introducen, en los cuales se enumeran los archivos encontrados con la ruta de acceso/nombre de archivo completos, la fecha y la hora del último acceso, el tamaño en bytes, el propietario y el nombre de archivo.
    - ✓ Los archivos de resultados se crean en la carpeta #agenttemp# definida en el paso 1.
    - ✓ El nombre del archivo de registro TXT se define por medio de la variable #logfile# en el paso 2.
    - ✓ El nombre del archivo CSV se define por medio de la variable #csvfile# en el paso 3.
    - ✓ Las máscaras de archivos se definen por medio de la variable #filemasks# en el paso 4.
    - ✓ Ambos archivos de resultados se cargan en el servidor Kaseya Server para su revisión y análisis en la carpeta Documentos del perfil de esas máquinas.
    - ✓ Además, el archivo de registro TXT se escribe en el registro de script para la elaboración de informes.
    - ✓ Este script también puede admitir alertas por cambios en los archivos por medio de la modificación de los pasos.
- **Audit Files (PST and OST)**

- Busca todos los archivos PST/OST por medio de un conjunto de máscaras de archivos y crea un archivo de registro TXT simple y un archivo CSV en el cual se enumeran los archivos encontrados con la ruta de acceso/nombre de archivo completos, la fecha y la hora del último acceso, el tamaño en bytes, el propietario y el nombre de archivo.
  - ✓ Los archivos de resultados se crean en la carpeta #agenttemp# definida en el paso 1.
  - ✓ El nombre del archivo de registro TXT se define por medio de la variable #logfile# en el paso 2.
  - ✓ El nombre del archivo CSV se define por medio de la variable #csvfile# en el paso 3.
  - ✓ Las máscaras de archivos se definen por medio de la variable #filemasks# en el paso 4.
  - ✓ Ambos archivos de resultados se cargan en el servidor Kaseya Server para su revisión y análisis en la carpeta Documentos del perfil de esas máquinas.
  - ✓ Además, el archivo de registro TXT se escribe en el registro de script para la elaboración de informes.
  - ✓ Este script también puede admitir alertas por cambios en los archivos por medio de la modificación de los pasos.

- **Audit Internet Speed (WEB100CLT)**
  - Usa la utilidad de clientes NDT para Windows (web100clt.exe). Se conecta al Servidor NDT público al cual accedió en el momento de ejecutar o programar el procedimiento (consulte http://e2epi.internet2.edu/ndt/ndt-server-list.html para obtener una lista de los servidores) y lleva a cabo una prueba de velocidad de Internet (carga/descarga) y otros diagnósticos de red. El archivo de resultados (Internet_Speed.txt) se recupera y se envía a la carpeta GetFile() del sistema.
- **Audit IRPStackSize Registry Key**
  - Audita el valor IRPStackSize. El ID de evento 2011 puede ser provocado por un antivirus y por otros tipos de software. Consulte http://support.microsoft.com/kb/177078.
- **Auditorear Cuentas de Admin Locales**
  - Introduce en el registro de procedimientos de agente las cuentas del usuario que son parte del grupo de Administradores en la máquina local.
- **Audit Local Guest Accounts**
  - Introduce en el registro de procedimientos de agente las cuentas del usuario que son parte del grupo de Invitados en la máquina local. Si las cuentas se mencionan en el informe, son habilitadas.
- **Audit Local User Accounts**
  - Introduce en el registro de procedimientos de agente las cuentas de usuarios definidas en la máquina.
- **Audit MP3 File Count**
  - Calcula la cantidad de archivos MP3 en la unidad C: de la máquina y escribe una entrada en el registro de procedimientos de agente en la cual se indica dicha cantidad.
- **Audit Open and Listening TCP Ports**
  - Audita puertos TCP abiertos y de audición en Windows por medio de NETSTAT y, a continuación, recupera los resultados y los envía a la carpeta GetFile() del sistema.
- **Audit PageFile Locations**
  - Audita las ubicaciones del archivo de paginación en los equipos Windows y escribe una entrada en el registro de procedimientos de agente con la información.
- **Audit Running Services (NET START)**
  - Audita los servicios que se encuentran en ejecución en un equipo Windows, recupera una lista de esos servicios y la envía a la carpeta GetFile() del sistema.
- **Audit Services (SC QUERY)**

- Audita la lista de Servicios de Windows por medio de SC QUERY, genera un archivo y lo recupera para enviarlo a la carpeta GetFile() del sistema.

- **Audit Services Registry Key**
  - Usa el comando REG para consultar la clave del registro HKLM\System\CurrentControlSet\Services de un agente, recupera los resultados y los envía a la carpeta GetFile() del sistema.
- **Auditorear clave de registro de desinstalación**
  - Usa el comando REG para consultar la clave del registro HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall de una máquina, recupera los resultados y los envía a la carpeta GetFile() del sistema.
- **Audit USB Plug-N-Play Devices**
  - Usa VBS y WMI (clase Win32_PnPEntity) para auditar los dispositivos USB en un equipo Windows. Los resultados recuperados se envían a la carpeta GetFile() del sistema.
- **Audit User Video Resolution**
  - Usa VBS para auditar la configuración actual de la resolución de pantalla de video. Escribe el resultado en el registro de procedimientos de agente y en el campo personalizado de información del sistema llamado Resolución de video del usuario.
- **Audit Windows Monitor Info**
  - Usa VBS y WMI (clase root\CIMV2:Win32_DesktopMonitor) para auditar la información de supervisión de Windows. Escribe los resultados en un archivo, lo recupera y lo envía a la carpeta GetFile() del sistema.
- **Audit Windows Monitor EDID Info**
  - Usa un VBS con WMI para detectar la información EDID del monitor (fabricante, modelo y número de serie del monitor) y la escribe en el registro de procedimientos de agente y en los campos personalizados de información del sistema.

Core.1 Windows Procedures.Desktops.Auditing.Share y NTFS

- **Audit All Share Sessions and Users (NET SESSION)**
  - Usa NET SESSION para volcar una lista básica de las sesiones existentes para los recursos compartidos en un agente y la carga a la carpeta Docs\Shares-NTFS, a fin de que los archivos puedan visualizarse mediante la pestaña Resumen de máquina, función Documentos.
- **Audit All Shared Files Opened and Users (NET FILE)**
  - Usa NET FILE para volcar una lista básica de los archivos abiertos para todos los recursos compartidos en un agente y la carga a la carpeta Docs\Shares-NTFS, a fin de que los archivos puedan visualizarse mediante la pestaña Resumen de máquina, función Documentos.
- **Audit All Shares (NET SHARE)**
  - Usa NET SHARE para volcar una lista básica de los recursos compartidos en un agente y la carga a la carpeta Docs\Shares-NTFS, a fin de que los archivos puedan visualizarse mediante la pestaña Resumen de máquina, función Documentos.
- **Audit Effective User/Group Fldr Perms (ACCESSCHK)**
  - Usa ACCESSCHK de Microsoft SysInternals para comprobar los permisos vigentes de un objeto de grupo o usuario basado en dominio o de una computadora local para acceder a una carpeta. Edite este script en los pasos 2 a 6 para obtener estas variables:

    pcdom = nombre de equipo o nombre de dominio del usuario o grupo
    usrgrp = nombre de usuario o de grupo para evaluar
    drive = letra de unidad en la cual se encuentra la carpeta
    folder = ruta de acceso completa de la carpeta para auditar
    fldrdesc = nombre descriptivo de la carpeta para auditar (sin caracteres especiales)
- **Audit Non-Admin Shares (SRVCHECK)**

- Usa SRVCHECK para volcar una lista básica de los recursos compartidos no administrativos que usa un agente y la carga a la carpeta Docs\Shares-NTFS, a fin de que los archivos puedan visualizarse mediante la pestaña Resumen de máquina, función Documentos.

- **Audit Shared Folders (DUMPSEC)**
  - Usa DUMPSEC para crear un informe de todos los recursos compartidos, sus rutas de acceso, cuentas, propietarios y permisos de acceso, y la carga a la carpeta Docs\Shares-NTFS, a fin de que los archivos puedan visualizarse mediante la pestaña Resumen de máquina, función Documentos.
- **Audit Shared Folders and ACLs (VBS/WMI)**
  - Usa VBS con WMI para auditar todos los recursos compartidos locales y los permisos NTFS y de recursos compartidos.
- **Audit Shared Printers (DUMPSEC)**
  - Usa DUMPSEC para crear un informe con todas las impresoras, sus nombres, cuentas, propietarios y permisos de acceso, y la carga a la carpeta Docs\Shares-NTFS, a fin de que los archivos puedan visualizarse mediante la pestaña Resumen de máquina, función Documentos.

Core.1 Windows Procedures.Desktops.Auditing.Share and NTFS.Audit Admin Shares

- **Audit Automatic Admin Shares**
  - Usa NET SHARE para auditar los recursos compartidos administrativos automáticos tales como C$, etc. Los resultados recuperados se envían a la carpeta del sistema Documentos, en la subcarpeta Share-NTFS.
- **Audit Automatic Admin Shares Setting**
  - Según el SO de la máquina, revisa el Registro de Windows para determinar si existe AutoShareServer o AutoShareWkst y cuáles son sus valores. Luego escribe una entrada en el registro de procedimientos de agente, la cual indica si esta característica está habilitada o no.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.Dell

- **Inventory Dell BIOS Settings via DCCU**
  - Usa la utilidad de configuración de clientes de Dell (DCCU) para realizar un inventario del BIOS de una máquina Dell de clase empresarial. Los resultados recuperados se envían a la carpeta GetFile() del sistema.
- **Set Dell BIOS Settings via DCCU**
  - Establece la configuración del BIOS de Dell según la configuración y el valor proporcionados en la programación. El formato de la configuración proporcionada del BIOS de Dell debe ser aquel que utiliza la utilidad de configuración de clientes de Dell (DCCU).

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.HP

- **HP BiosConfigUtility GetConfig**
  - Usa la utilidad de configuración del BIOS de HP para realizar un inventario del BIOS de una máquina HP de clase empresarial. Los resultados recuperados se envían a la carpeta GetFile() del sistema.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.Lenovo

- **Get Lenovo BIOS Settings via WMI-VBS**
  - Usa VBS y WMI para obtener la configuración completa del BIOS de los sistemas Lenovo.
- **Set Lenovo BIOS Settings via WMI-VBS**

- Usa VBS y WMI para establecer la configuración del BIOS en los sistemas Lenovo. Solicita el nombre y el valor de la configuración del BIOS de Lenovo en el momento de su ejecución o programación.

Core.1 Windows Procedures.Desktops.Machine Control.File Sharing

- **Disable Simple File Sharing (Sets ForceGuest=0) on Windows XP**
  - Deshabilita la característica de uso compartido simple de archivos en los sistemas Windows XP (establece ForceGuest=0). A continuación, detiene y reinicia el servicio del servidor para que se implemente el cambio.
- **Enable Automatic Admin Shares**
  - Habilita la característica AutoShareWks en las estaciones de trabajo Windows, a fin de que los recursos compartidos administrativos se generen de manera automática al iniciarse el servicio del servidor. Este procedimiento de agente NO reinicia el servicio del servidor (LanmanServer).
- **Enable Simple File Sharing (Sets ForceGuest=1) on Windows XP**
  - Habilita la característica de uso compartido simple de archivos en los sistemas Windows XP (ForceGuest=1). A continuación, detiene y reinicia el servicio del servidor para que se implemente el cambio.
- **Disable Automatic Admin Shares**
  - Deshabilita la característica AutoShareWks en las estaciones de trabajo Windows, a fin de que los recursos compartidos administrativos se generen de manera automática al iniciarse el servicio del servidor. Este procedimiento de agente NO reinicia el servicio del servidor (LanmanServer).

Core.1 Windows Procedures.Desktops.Machine Control.File System

- **Convert File System on Drive to NTFS**
  - Convierte el formato del sistema de archivos de la unidad del sistema (es decir, la partición de arranque) de FAT/FAT32 a NTFS. Esto sólo funciona en aquellos sistemas operativos que admiten el formato NTFS (Windows NT4/2000/XP/2003/Vista).
- **Delete Files Based on Modified Date**
  - Solicita la antigüedad de los archivos que se van a eliminar, la unidad/ruta de acceso completa para comenzar con la operación de eliminación y la máscara de archivo que se va a eliminar. Luego usa FORFILES para procesar recursivamente todas las carpetas en la unidad/ruta de acceso completa introducida y elimina los archivos que coinciden con la máscara de archivo si su antigüedad es superior a la indicada.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Block Websites

- **Bloquear "todos" los sitios Web**
  - Este script edita el archivo de hosts de Windows y redirige al usuario al localhost cuando este intente acceder a cualquier sitio web en el símbolo del sistema, es decir que bloquea el acceso al sitio web desde ese extremo. Esto puede ser útil para los empleadores que intentan mejorar la productividad o simplemente, bromear.
- **Borrar todos los sitios web bloqueados**
  - Se usa para quitar todas las ediciones del archivo de hosts de Windows. Actualiza la configuración predeterminada del archivo de hosts.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Diagnostics

- **Network Diagnostics Test (NETSH)**
  - Usa NETSH para llevar a cabo una prueba de diagnóstico de red, recupera los resultados y los envía a la subcarpeta Diagnósticos de red que se encuentra en la carpeta del sistema Documentos.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Network Connection

- **Configure Local Area Connection to Utilize DHCP**
  - Usa NETSH para modificar la configuración de la conexión de red de Windows con nombre llamada “Conexión de área local” y así poder usar la dirección IP y la configuración de DNS y WINS del DHCP.
- **Fix RAS DNS Priority**
  - Soluciona el problema relacionado con la prioridad de enlace de DNS de un RAS, el cual se describe en http://support.microsoft.com/kb/311218/en-us.
- **Get Windows IP Configuration (IPCONFIG /ALL)**
  - Usa IPCONFIG /ALL para obtener la configuración de dirección IP de todas las conexiones de red habilitadas en un equipo Windows. Los resultados recuperados se envían a la carpeta GetFile() del sistema.
- **Release and Renew IP Address**
  - Usa un archivo por lotes para liberar y renovar la dirección IP de los equipos Windows.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Dell

- **Enable Wake-On-LAN in Dell BIOS (DCCU)**
  - Usa la utilidad de configuración de clientes de Dell (DCCU) para habilitar Wake On LAN en el BIOS de las máquinas Dell de clase empresarial.
- **Enable Wake-On-LAN in Dell BIOS (CCTK)**
  - Usa la aplicación Client Configuration Tool Kit (CCTK) de Dell para habilitar Wake On LAN en el BIOS de las máquinas Dell de clase empresarial.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.HP

- **Enable Wake-On-LAN in HP BIOS**
  - Usa la utilidad de configuración del BIOS de HP para habilitar Wake On LAN en el BIOS de las máquinas HP de clase empresarial.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Lenovo

- **Enable Wake-On-LAN in Lenovo BIOS**
  - Usa VSB y WMI para habilitar Wake On LAN en el BIOS de las máquinas Lenovo de clase empresarial.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Windows

- **Enable Wake-On-LAN In Windows for all NICs**
  - Usa VBS para habilitar la característica Wake On LAN de administración de energía en cada interfaz de red de Windows. Esto permite que la máquina se reactive por medio de Magic Packet cuando está suspendida o en hibernación. Las características de WOL dentro del BIOS también deben estar habilitadas para que WOL funcione.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wireless

- **Disable Wireless Networking Devices**
  - Usa DEVCON.EXE para deshabilitar los dispositivos de red inalámbricos en un sistema Windows.
- **Enable Wireless Networking Devices**
  - Usa DEVCON.EXE para habilitar los dispositivos de red inalámbricos en un sistema Windows.
- **Disable NIC on Wireless Network Connection**
  - Usa NETSH para deshabilitar la NIC asociada a la conexión de red de Windows con nombre llamada “Conexión de red inalámbrica”.

- **Enable NIC on Wireless Network Connection**
  - Usa NETSH para habilitar la NIC asociada a la conexión de red de Windows con nombre llamada “Conexión de red inalámbrica”.

Core.1 Windows Procedures.Desktops.Machine Control.Reboot/Shutdown

- **Hibernate Now**
  - Lleva a un equipo Windows a un estado de hibernación de manera inmediata.
- **Suspend Now**
  - Lleva a un equipo Windows a un estado de suspensión de manera inmediata.
- **Shutdown Abort**
  - Apagar la computadora usando Shutdown.exe
- **Shutdown in 60 Seconds**
  - Apaga la computadora en 60 segundos por medio de Shutdown.exe.
- **Lock Desktop**
  - Bloquea el escritorio de un equipo Windows y solicita las credenciales al usuario que se encuentra conectado actualmente para desbloquearlo.

Core.1 Windows Procedures.Desktops.Machine Control.System Restore

- **List All System Restore Points**
  - Usa WMIC para enumerar todos los puntos de restauración del sistema, genera una lista y la recupera para enviarla a la carpeta GetFile() del sistema.
- **Enable System Restore on All Drives**
  - Usa DISKPART para enumerar todas las particiones locales y luego envía esta lista de unidades a WMIC para deshabilitar la opción Restaurar sistema en cada volumen. Esto quita todos los puntos de restauración del sistema existentes.
- **Disable System Restore All Drives**
  - Usa DISKPART para enumerar todas las particiones locales y luego envía esta lista de unidades a WMIC para deshabilitar la opción Restaurar sistema en cada volumen. Esto quita todos los puntos de restauración del sistema existentes.
- **Create a Named System Restore Point**
  - Usa WMIC para crear un punto de restauración del sistema.

Core.1 Windows Procedures.Desktops.Machine Control.Trusted Sites

- **Agregar Sitios Confiables**
  - Ejecuta un procedimiento de registro en la máquina para permitir que cualquier cosa del dominio ejecute ActiveX. En este ejemplo, agrega Kaseya.net.

Core.1 Windows Procedures.Desktops.Machine Control.USB/Disk Drive Control

- **Deshabilitar Controladores USB**
  - **Debe reiniciar la máquina extremo después de realizar cambios por medio de un script**. Existe un simple cambio de registro que evitará que los controladores de almacenamiento USB se inicien cuando el sistema arranque. Evita tener que ir hasta una computadora y copiar los datos de una llave USB, pero permite que el escáner, el teclado y el mouse sigan funcionando.
  - Como siempre, realice una copia de seguridad del sistema antes para evitar inconvenientes con el registro. Simplemente abra regedit y busque la siguiente clave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor. Verifique el valor de ‘Start’ (Inicio). Cambie este valor a 4, y los dispositivos de almacenamiento USB se deshabilitarán. Si cambia ese valor a 3, dichos dispositivos se habilitarán.
- **Habilitar unidades USB**

- **Debe reiniciar la máquina extremo después de realizar cambios por medio de un script**. Existe un simple cambio de registro que evitará que los controladores de almacenamiento USB se inicien cuando el sistema arranque. Evita tener que ir hasta una computadora y copiar los datos de una llave USB, pero permite que el escáner, el teclado y el mouse sigan funcionando.
- Como siempre, realice una copia de seguridad del sistema antes para evitar inconvenientes con el registro. Simplemente abra regedit y busque la siguiente clave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor. Verifique el valor de 'Start' (Inicio). Cambie este valor a 4, y los dispositivos de almacenamiento USB se deshabilitarán. Si cambia ese valor a 3, dichos dispositivos se habilitarán.

- **Disable USB Drives Write Protection**
  - Deshabilita la protección de escritura de los dispositivos USB en los equipos Windows que operan con Windows XP SP2 o sistemas operativos superiores (consulte http://technet.microsoft.com/en-us/library/bb457157.aspx).
- **Enable USB Drives Write Protection**
  - Habilita la protección de escritura de los dispositivos USB en los equipos Windows que operan con Windows XP SP2 o sistemas operativos superiores (consulte http://technet.microsoft.com/en-us/library/bb457157.aspx).
- **Disable CD-ROM Drives**
  - Deshabilita los dispositivos de discos CD-ROM.
- **Enable CD-ROM Drives**
  - Habilita los dispositivos de discos CD-ROM.
- **Disable High Capacity Floppy Drives**
  - Deshabilita los dispositivos de disquete de alta capacidad.
- **Enable High Capacity Floppy Drives**
  - Habilita los dispositivos de disquete de alta capacidad.
- **Disable Floppy Disk Drives**
  - Deshabilita los dispositivos de disquete.
- **Enable Floppy Disk Drives**
  - Habilita los dispositivos de disquete.
- **Restrict Desktop Access**
  - Restringe el acceso al Escritorio en Explorer. El Escritorio aparecerá vacío y los usuarios no podrán usarlo ni acceder a él.
- **Unrestrict Desktop Access**
  - Restringe el acceso al Escritorio en Explorer. El Escritorio aparecerá vacío y los usuarios no podrán usarlo ni acceder a él.
- **Hide and Restrict Access to All Drives (A-Z) in Explorer**
  - Usa la configuración del registro NoViewOnDrive y NoDrives para ocultar y restringir el acceso a todas las letras de unidad, de la A a la Z, en un equipo Windows.
- **Hide and Restrict Access to C and D Drives in Explorer**
  - Es posible elegir entre "Bloquear sólo C", "Bloquear sólo D" o "Bloquear todas las unidades" con uno de los procedimientos "01.Block".
- **Hide and Restrict Access to Any List of Drives in Explorer**
  - Es posible elegir entre "Bloquear sólo C", "Bloquear sólo D" o "Bloquear todas las unidades" con uno de los procedimientos "01.Block".
- **Unhide and Unrestrict Access to All Drives (A-Z) in Explorer**
  - Elimina las restricciones previas de acceso a las unidades que pudieran existir.

- Nota: Windows permite bloquear el acceso para ver distintas letras de unidad dentro de Explorer. Esta restricción evita que los usuarios utilicen Mi PC o Explorer para acceder al contenido de las unidades seleccionadas. A su vez, no se les permite utilizar los comandos Ejecutar, Conectar a unidad de red o Dir para visualizar los directorios en esas unidades. Este procedimiento de agente elimina toda restricción a tal efecto.

Core.1 Windows Procedures.Desktops.Machine Control.User Access Control

- **Set User Access Control (UAC) to Always Notify**
  - Establece el control de acceso de usuarios en Notificarme siempre en Windows Vista, Windows 7 y Windows 8.
- **Set User Access Control (UAC) to Default Notify**
  - Establece el control de acceso de usuarios en Notificarme de manera predeterminada en Windows Vista, Windows 7 y Windows 8.
- **Set User Access Control (UAC) to Insecure Notify**
  - Establece el control de acceso de usuarios en Notificarme sólo en algunos casos en Windows Vista, Windows 7 y Windows 8.
- **Set User Access Control (UAC) to Never Notify**
  - Deshabilita el control de acceso de usuarios en Windows Vista, Windows 7 y Windows 8.

Core.1 Windows Procedures.Desktops.Machine Control.Windows Configuration

- **Hide an Account from Windows Fast User Switching Logon Screen**
  - Este script agrega un valor DWORD con el valor de “usuario de soporte” y datos a 0. Después de reiniciar, la computadora ya no mostrará el “usuario de soporte” en la pantalla de inicio de sesión.
- **Unhide an Account from Windows Fast User Switching Logon Screen**
  - Este script agrega un valor DWORD con el valor de “usuario de soporte” y datos a 0. Después de reiniciar, la computadora ya no mostrará el “usuario de soporte” en la pantalla de inicio de sesión.
- **Disable Show Hidden Operating System Files**
  - Deshabilita la opción Mostrar archivos ocultos del sistema operativo en Windows Explorer.
- **Enable Display the Contents of System Folders**
  - Habilita la opción Mostrar contenido de carpetas del sistema en Windows Explorer.
- **Enable Hide Extensions for Known File Types**
  - Habilita la opción Ocultar extensiones de tipos de archivo conocidos en Windows Explorer.
- **Enable Show Hidden Files and Folders**
  - Habilita la opción Mostrar carpetas y archivos ocultos en Windows Explorer.
- **Enforce Windows Minimum Password Length of 8 Characters**
  - Puede forzar Windows a rechazar contraseñas que no cumplan con una longitud mínima. Esto es útil para que las personas no utilicen contraseñas triviales cuando la seguridad es un problema. Agregar un nuevo valor REG_BINARY de "MinPwdLen", y fijar los datos en el número mínimo de caracteres requeridos para que una contraseña sea aceptada. El siguiente ejemplo es 8. Nota: Esto no afecta a las contraseñas existentes, sólo a una nueva o cambiada.
- **Suppress Balloon Pop-Ups for Current Windows User**
  - Suprime todos los globos emergentes en Windows para el usuario conectado actualmente. Consulte http://msdn.microsoft.com/en-us/library/ms940877(v=winembedded.5).aspx.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Check Disk

- **Check Disk All Drives**

- Usa DISKPART para enumerar todas las particiones locales y luego envía esta lista de unidades a CHKDSK para reparar cada volumen.

- **Check Disk System Drive (Schedule at Next Restart)**
  - Ejecuta un comando CHKDSK en la unidad del sistema. Los resultados del mantenimiento se evalúan por medio del script Check Disk Verify.
- **Check Disk System Drive (Analysis Only)**
  - Ejecuta un comando CHKDSK en la unidad del sistema. Se evalúan los resultados del mantenimiento y se escribe una entrada en el registro de procedimientos de agente con los resultados, los cuales se recuperan y se envían a la carpeta GetFile() del sistema.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Defragmentation

- **Defragment All Drives**
  - Usa DISKPART para enumerar todas las particiones locales y luego envía esta lista de unidades a DEFRAG para optimizar cada volumen. Recupera los resultados de DEFRAG correspondientes a todas las unidades y los envía a la carpeta GetFile() del sistema.
- **Defragment System Drive (Analysis Only)**
  - Realiza un análisis de desfragmentación en la unidad del sistema en Windows (en general, en la unidad C:). Los resultados de la desfragmentación se escriben en el registro de procedimientos de agente.
- **Defragment Page File & Registry**
  - Usa la utilidad PageDefrag de Sysinternals para desfragmentar el registro y el archivo de paginación del sistema, y luego reiniciar (sólo Windows XP).
- **Defragment System Drive (Analysis & Prompt User If Reqd)**
  - Realiza un análisis de desfragmentación en la unidad del sistema en Windows (en general, en la unidad C:). Los resultados de la desfragmentación se escriben en el registro de procedimientos de agente. Si un usuario inició sesión en la máquina, el procedimiento brinda la opción de ejecutar una desfragmentación completa en la unidad y la lleva a cabo si se el usuario responde afirmativamente.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Disk Cleanup

- **Windows Disk Cleanup**
  - Establece las entradas de registro “sageset” para cleanmgr.exe y, a continuación, ejecuta cleanmgr.exe con el parámetro “sagerun” para que borre automáticamente los archivos en las ubicaciones siguientes: Carpeta Temporal de Configuración Activa, Limpiador Indexador de Contenido, Archivos de Programas Descargados, Archivos Caché de Internet, Archivos de Volcado de Memoria, Archivos ChkDsk Viejos, Archivos Caché de Escritorio Remotos, Archivos de Registro de Configuración, Archivos Temporales, Archivos Fuera de Línea Temporales, Caché de WebClient y WebPublisher

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Flush DNS

- **Flush DNS Resolver Cache**
  - Vacía y restablece el contenido de la memoria caché de resolución de clientes DNS ejecutando IPCONFIG /FLUSHDNS.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.IE Files Management

- **Borrar cookies de Internet Explorer**
  - Borra las cookies de Internet Explorer correspondientes al usuario que está conectado.
- **Borrar datos de formulario de Internet Explorer**

- Borra los datos de formularios de Internet Explorer correspondientes al usuario que está conectado.

- **Borrar historial de Internet Explorer**
  - Borra el historial de Internet Explorer correspondientes al usuario que está conectado.
- **Borrar contraseñas de Internet Explorer**
  - Borra las contraseñas de Internet Explorer correspondientes al usuario que está conectado.
- **Borrar archivos temporales de Internet Explorer**
  - Borra los archivos temporales de Internet Explorer correspondientes al usuario que está conectado.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore

- **Create Weekly Desktop Maintenance System Restore Point**
  - Usa WMIC para crear un punto de restauración del sistema llamado Mantenimiento semanal de escritorio. Es posible recurrir a este procedimiento de agente al principio del Procedimiento de mantenimiento semanal de estaciones de trabajo.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore

- **Create Patch Management System Restore Point**
  - Usa WMIC para crear un punto de restauración del sistema llamado Administración de parches. Se puede recurrir a este procedimiento de agente antes de la implementación de un parche por medio de un Procedimiento previo de agente para actualización automática.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.TEMP Files

- **Clear User TEMP Folder**
  - Elimina todos los archivos y carpetas dentro de la carpeta %TEMP% de los usuarios que iniciaron sesión que no se encuentran actualmente abiertos o bloqueados por Windows.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Time Sync

- **Synchronize Time via SNTP**
  - Fija el reloj de Windows para recuperar le hora desde time.windows.com

Core.1 Windows Procedures.Desktops.Maintenance.Desktop Maintenance

- **Workstation Weekly Maintenance**
  - Ejecuta todas las tareas de mantenimiento semanal de escritorio; programe este script para que se ejecute durante el período de mantenimiento.

Core.1 Windows Procedures.Desktops.Maintenance.Maintenance Notifications

- **Weekly Desktop Maintenance Reminder**
  - Este script está diseñado para ejecutarse durante el día, antes del mantenimiento de la aplicación de parches para escritorio. Enviará un mensaje al usuario final del escritorio en el cual se le indicará que no debe usar la máquina por la noche.

Core.1 Windows Procedures.Desktops.Software Control.Internet Explorer

- **Set Default Internet Explorer Home Page**
  - Fijar Página predeterminada en Internet Explorer. Sólo cambiar el sitio en el paso 1.

Core.1 Windows Procedures.Desktops.Software Control.Windows Firewall

- **Disable Windows Firewall**
  - Usa NETSH para deshabilitar el firewall de Windows.

Core.1 Windows Procedures.Servers.Active Directory.AD Replication

- **Perform an AD Replication Check Using REPADMIN**
  - Ejecuta una comprobación de replicación de los servicios de Active Directory con la utilidad REPADMIN. Envía los resultados por correo electrónico, por lo que DEBE actualizar la dirección de correo para poder recibirlos.

Core.1 Windows Procedures.Servers.Exchange.Exchange Best Practices Analyzer.Exchange 2003

- **ExBPA Report 2003 server**
  - Diseñado para Exchange 2003. Usa el analizador de procedimientos recomendados de Exchange, a fin de generar un informe de los errores. MS Logparser 2.0 luego se usa para analizar los resultados y enviar un informe final por correo electrónico a la dirección del administrador que ejecuta o programa el procedimiento de agente. El analizador de procedimientos recomendados de Exchange debe instalarse para poder usar este procedimiento de agente.

Core.1 Windows Procedures.Servers.Exchange.Exchange Best Practices Analyzer.Exchange 2007

- **ExBPA Report 2007 server**
  - Diseñado para Exchange 2007. Usa el analizador de procedimientos recomendados de Exchange, a fin de generar un informe de los errores. MS Logparser 2.0 luego se usa para analizar los resultados y enviar un informe final por correo electrónico a la dirección del administrador que ejecuta o programa el procedimiento de agente. El analizador de procedimientos recomendados de Exchange debe instalarse para poder usar este procedimiento de agente.

Core.1 Windows Procedures.Servers.IIS Server

- **Perform an IISRESET on IIS Server**
  - Realiza un IISRESET en una máquina.

Core.1 Windows Procedures.Servers.Maintenance

- **Weekly Server Maintenance**
  - Ejecuta todas las tareas de mantenimiento semanal del escritorio.

Core.1 Windows Procedures.Servers.Monitoring Remediation.Disk Usage

- **DiskUsage.GetDirTree.C-D-E-F-G-M-N**
  - Devuelve uso de disco en las unidades C, D, E, F, G, M y N. Escribe los resultados del árbol de uso de disco en el registro de procedimientos de agente. Las unidades que no existen no mostrarán ningún resultado de uso de disco.

Core.1 Windows Procedures.Servers.Monitoring Remediation.Get Process List

- **Rendimiento. Obtener lista de procesos**
  - Usa kperfmon.exe para obtener la lista de procesos, % de CPU y consumo de memoria. Este script puede estar configurado para ejecutarse cuando los contadores de rendimiento de monitor disparan una alarma. Escribe los resultados en el registro de procedimientos de agente.

Core.1 Windows Procedures.Servers.Print Server

- **Clear Print Spooler Queues**
  - Detiene el administrador de trabajos de impresión, elimina las colas y lo reinicia.

Core.1 Windows Procedures.Servers.Service Control Manager

- **Compilar SCM**
  - Vuelve a compilar el Administrador de control de servicios para verificar que los eventos de este figuren en el registro del sistema.

Core.1 Windows Procedures.Servers.Terminal Server

- **Terminal Server - Logoff Disconnected Sessions**
  - Cierra todas las sesiones desconectadas en un servidor Terminal Server.
- **Terminal Server - Logoff Session X**
  - URL de referencia: http://technet2.microsoft.com/windowsserver/en/library/26b3946e-5dbc-4248-9ea4-5adaae45b81f1033.mspx?mfr=true
- **Servidor de terminal - Desconectar sesión 1**
  - URL de referencia: http://technet2.microsoft.com/windowsserver/en/library/26b3946e-5dbc-4248-9ea4-5adaae45b81f1033.mspx?mfr=true
- **Terminal Server - Query Sessions**
  - Usa QUERY USER para generar una lista de todas las sesiones de un servidor Terminal Server y escribe la lista de información de sesión en el registro de procedimientos de agente.
- **Terminal Server - Reboot in 60 Seconds**
  - Reinicia un servidor Terminal Server después de darles a los usuarios conectados 60 segundos para cerrar las aplicaciones y guardar sus trabajos.
- **Terminal Server - Shutdown in 60 Seconds**
  - Apaga un servidor Terminal Server después de darles a los usuarios conectados 60 segundos para cerrar las aplicaciones y guardar sus trabajos.

Core.2 Macintosh Procedures

Core.2 Macintosh Procedures.Machine Control.Auditing

- **Collect HDD, User, Process, Network info**
  - Recopila algo de información sobre una Mac. También funciona en casi todas las distribuciones Linux, una vez que se admiten. Ejecuta DF (punto de montaje, información sobre el espacio en disco), uname -a (información sobre el SO), ls /users/ (información sobre los usuarios), ifconfig (información sobre la NIC), netstat (información sobre la conexión de red), ps aux (información sobre el proceso). Los resultados se envían a /tmp/macinfo.txt y luego se devuelven al servidor Kaseya Server. Se pueden encontrar en Auditaría > Documentos del agente.
- **Retrieve List of Disks and Email to Me**
  - Usa DISKUTIL para enumerar todos los discos Mac OS X, recupera la lista de discos y la envía a la carpeta GetFile() del sistema. Luego envía un correo electrónico al administrador que ejecutó o programó el procedimiento de agente.

Core.2 Macintosh Procedures.Machine Control.Monitoring

- **Check SMART Status of Disk0**
  - Usa DISKUTIL para obtener el estado de tecnología de supervisión automática, análisis y generación de informes (SMART) del Disk0 de la Mac y envía un correo electrónico al administrador que ejecutó o programó el procedimiento si el estado de SMART es Failing (Error).

Core.2 Macintosh Procedures.Machine Control.Networking

- **Bind Mac to an Active Directory Domain**
  - Usa DSCONFIGAD para asociar un sistema Mac OS X a un dominio de Active Directory. Solicita el nombre completo del dominio de AD, las credenciales de administrador de dicho dominio y la unidad organizativa (UO) de destino.

Core.2 Macintosh Procedures.Machine Control.System

- **Configure Mac Energy Saver Settings**
  - Establece la configuración de ahorro de energía en las preferencias del sistema Macintosh. Usa PMSRT para configurar el perfil del adaptador de energía (es decir, cuando la Mac recibe suministro de CA) de la siguiente manera: La pantalla se suspende después de 45 minutos de inactividad. La computadora se suspende después de 1 hora de inactividad.
- **Update Mac IP/Name Configuration Records.**
  - Usa CHANGEIP para fijar los cambios de IP/nombre en los servidores Mac OS X. Solicita el nombre anterior y el nombre nuevo. CHANGEIP se utiliza para actualizar de forma manual los registros de configuración cuando la dirección IP o el nombre de host de un servidor se modificaron de forma tal que los servicios afectados no pueden procesarse adecuadamente, por ejemplo, cuando un servidor se encuentra detrás de un dispositivo NAT y la identidad WAN cambió. En general, los administradores utilizan este comando para corregir los servicios afectados cuando se modifica la información de red del servidor. Es posible invocar CHANGEIP antes de la implementación del cambio. En tal caso, los argumentos consisten en las direcciones IP (actual y pendiente) del servidor y, opcionalmente, en el nombre de host existente y el nuevo.
- **Change Mac Computer Name**
  - Cambiar el nombre de Mac con SCUTIL.

Core.2 Macintosh Procedures.Machine ControlSystem Preferences.Energy Saver.Battery Profile

- **Energy Saver - Battery Set Auto Reduce Brightness Before Display Sleep Off**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento desactiva la opción “Reducir automáticamente el brillo antes del reposo de la pantalla”.
- **Energy Saver - Battery Set Auto Reduce Brightness Before Display Sleep On**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento activa la opción “Reducir automáticamente el brillo antes del reposo de la pantalla”.
- **Energy Saver - Battery Set Computer Sleep 120 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 120 minutos.
- **Energy Saver - Battery Set Computer Sleep 15 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 15 minutos.
- **Energy Saver - Battery Set Computer Sleep 30 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 30 minutos.
- **Energy Saver - Battery Set Computer Sleep 45 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 45 minutos.

- **Energy Saver - Battery Set Computer Sleep 60 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 60 minutos.
- **Energy Saver - Battery Set Computer Sleep 90 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 90 minutos.
- **Energy Saver - Battery Set Display Sleep 120 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 120 minutos.
- **Energy Saver - Battery Set Display Sleep 15 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 15 minutos.
- **Energy Saver - Battery Set Display Sleep 30 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 30 minutos.
- **Energy Saver - Battery Set Display Sleep 45 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 45 minutos.
- **Energy Saver - Battery Set Display Sleep 60 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 60 minutos.
- **Energy Saver - Battery Set Display Sleep 90 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 90 minutos.
- **Energy Saver - Battery Set Hard Disk(s) to Sleep When Possible Off**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento desactiva la opción “Poner el disco en reposo cuando sea posible”.
- **Energy Saver - Battery Set Hard Disk(s) to Sleep When Possible On**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento activa la opción “Poner el disco en reposo cuando sea posible”.
- **Energy Saver - Battery Set Hibernation Mode 0 (Wake from Memory)**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el modo de reposo 0 (salir del reposo desde la memoria).
- **Energy Saver - Battery Set Hibernation Mode 25 (Wake from Disk)**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el modo de reposo en 25 (salir del reposo desde el disco).
- **Energy Saver - Battery Set Hibernation Mode 3 (Wake from Memory or Disk)**

- Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento establece el modo de reposo 3 (salir del reposo desde la memoria o el disco).

- **Energy Saver - Battery Set Slightly Dim Display Off**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento desactiva la opción “Atenuar ligeramente la pantalla”.
- **Energy Saver - Battery Set Slightly Dim Display On**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil de batería en Preferencias del sistema de Mac. Este procedimiento activa la opción “Atenuar ligeramente la pantalla”.

Core.2 Macintosh Procedures.Machine Control.System Preferences.Energy Saver.Power Adapter Profile

- **Energy Saver - Power Adapter Set Auto Reduce Brightness Before Display Sleep Off**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento desactiva la opción “Reducir automáticamente el brillo antes del reposo de la pantalla”.
- **Energy Saver - Power Adapter Set Auto Reduce Brightness Before Display Sleep On**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento activa la opción “Reducir automáticamente el brillo antes del reposo de la pantalla”.
- **Energy Saver - Power Adapter Set Computer Sleep 120 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 120 minutos.
- **Energy Saver - Power Adapter Set Computer Sleep 15 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 15 minutos.
- **Energy Saver - Power Adapter Set Computer Sleep 30 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 30 minutos.
- **Energy Saver - Power Adapter Set Computer Sleep 45 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 45 minutos.
- **Energy Saver - Power Adapter Set Computer Sleep 60 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 60 minutos.
- **Energy Saver - Power Adapter Set Computer Sleep 90 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo del ordenador” en 90 minutos.
- **Energy Saver - Power Adapter Set Display Sleep 120 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 120 minutos.

- **Energy Saver - Power Adapter Set Display Sleep 15 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 15 minutos.
- **Energy Saver - Power Adapter Set Display Sleep 30 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 30 minutos.
- **Energy Saver - Power Adapter Set Display Sleep 45 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 45 minutos.
- **Energy Saver - Power Adapter Set Display Sleep 60 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 60 minutos.
- **Energy Saver - Power Adapter Set Display Sleep 90 Mins**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el “Reposo de la pantalla” en 90 minutos.
- **Energy Saver - Power Adapter Set Hard Disk(s) to Sleep When Possible Off**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento desactiva la opción “Poner el disco en reposo cuando sea posible”.
- **Energy Saver - Power Adapter Set Hard Disk(s) to Sleep When Possible On**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento activa la opción “Poner el disco en reposo cuando sea posible”.
- **Energy Saver - Power Adapter Set Hibernation Mode 0 (Wake from Memory)**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el modo de reposo 0 (salir del reposo desde la memoria).
- **Energy Saver - Power Adapter Set Hibernation Mode 25 (Wake from Disk)**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el modo de reposo en 25 (salir del reposo desde el disco).
- **Energy Saver - Power Adapter Set Hibernation Mode 3 (Wake from Memory or Disk)**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento establece el modo de reposo 3 (salir del reposo desde la memoria o el disco).
- **Energy Saver - Power Adapter Set Wake for AirPort Network Access Off**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento desactiva la opción “Activar el ordenador para permitir el acceso a la red AirPort”.
- **Energy Saver - Power Adapter Set Wake for AirPort Network Access On**
  - Utiliza PMSET para configurar los parámetros del economizador para el perfil del adaptador de corriente en Preferencias del sistema de Mac. Este procedimiento activa la opción “Activar el ordenador para permitir el acceso a la red AirPort”.

Core.2 Macintosh Procedures.Machine Control.System Preferences.Security

- **Security - General Set Disable Automatic Login On**
  - Utiliza DEFAULTS para configurar los parámetros de seguridad para el panel General en Preferencias del sistema de Mac. Este procedimiento activa la opción “Desactivar el inicio de sesión automático” y quita la información de cuenta existente para el inicio de sesión automático.

Core.2 Macintosh Procedures.Machine Control.Utils

- **Reiniciar acoplamiento de SO X**
  - Reinicia el Dock de Mac.
- **Send a Text To Speech Message to OS X**
  - Utiliza OSASCRIPT y SAY para reproducir el mensaje introducido mediante el audio de la Mac (es decir, texto a voz).
- **Take a Camera Picture on OS X**
  - Usa el puerto “isightcapture” de Mac para tomar una fotografía con la cámara de una Mac.
- **Take a Screen Capture of Current Users OS X Desktop**
  - Realiza una captura la pantalla del escritorio actual de Mac OS X del usuario conectado. El archivo de la captura de pantalla se recupera y se envía a la carpeta Documentos del sistema en el servidor.

Core.2 Macintosh Procedures.Maintenance

- **Macintosh Weekly Maintenance**
  - Realiza una serie de tareas de mantenimiento de rutina en una máquina con Macintosh OS X.
- **General OS X House Cleaning**
  - Realiza una limpieza del sistema, elimina archivos de registro antiguos, archivos de trabajo y archivos basura, limpia las memorias caché de los usuarios y del sistema, rota los registros del sistema y de aplicaciones, y vuelve a generar la memoria caché DYLD y el índice Spotlight.
- **Verify and Repair OS X Disk Volumes**
  - Lleva a cabo operaciones de verificación y reparación de disco con DISKUTIL.
- **Repair OS X Disk Permissions**
  - Lleva a cabo una operación de permisos de reparación de disco con DISKUTIL.

Core.2 Macintosh Procedures.Software Update

- **Mac Software Update - Install All Updates and Alert If Any**
  - Actualización de software de Mac: instala TODAS las actualizaciones. Si se instalan nuevas actualizaciones, envía una alerta. Para obtener más detalles, consulte “Actualización de software de Mac: instalar todas las actualizaciones” en Informes -> Registros. Los detalles de los agentes se guardan en Auditar -> Documentos.
- **Mac Software Update - Install All Updates and Retrieve/Log Results**
  - Utiliza SOFTWAREUPDATE para instalar todas las actualizaciones de software de Mac.
- **Mac Software Update - Install All Updates and Reboot After**
  - Usa SOFTWAREUPDATE para instalar todas las actualizaciones de software de Mac y para reiniciar a continuación.
- **Mac Software Update - Retrieve and Email List of All Updates to Me**
  - Utiliza SOFTWAREUPDATE para generar un archivo con una lista de todas las actualizaciones de software de Mac, recuperarlo y enviarlo por correo electrónico a la dirección del usuario del VSA que ejecuta o programa el procedimiento.
- **Mac Software Update - Download All Updates and Alert If Any**

- Utiliza SOFTWAREUPDATE para descargar todas las actualizaciones de software de Mac y generar un archivo con una lista de ellas. En caso de que haya actualizaciones disponibles, recupera el archivo y genera una alerta.

- **Mac Software Update - Download Recommended Updates and Alert If Any**
  - Actualización software Mac - Descargar las actualizaciones recomendadas Si se descargan nuevas actualizaciones, envía una alerta. Para obtener más detalles, consulte "Actualización de software de Mac: descargar las actualizaciones recomendadas" en Informes -> Registros. Los detalles de los agentes se guardan en Auditar -> Documentos.
- **Mac Software Update - Install Recommended Updates and Retrieve/Log Results**
  - Utiliza SOFTWAREUPDATE para instalar las actualizaciones recomendadas de software de Mac.
- **Mac Software Update - Retrieve List of All Updates and Alert If Any**
  - Actualización de software de Mac: enumera TODAS las actualizaciones. Si se detectan nuevas actualizaciones, envía una alerta. Para obtener más detalles, consulte "Actualización de software de Mac: enumerar todas las actualizaciones" en Informes -> Registros. Los detalles de los agentes se guardan en Auditar -> Documentos.

Core.3 Linux Procedures

Core.3 Linux Procedures.Machine Control.Audit Info

- **Get Current Memory information**
  - Recupera información actual sobre disponibilidad de la memoria.
- **Get Linux and Kernel Version**
  - Recupera la versión actual de Linux (nombre) e información del núcleo.

Core.3 Linux Procedures.Machine Control.DNS

- **Create HOSTS File**
  - Este procedimiento crea un nuevo archivo HOSTS con las variables y la información provistas por usted.
- **Edit DNS Servers**
  - Edita los servidores DNS.
- **Set Hostname**
  - Este procedimiento establece el nombre de host de sus servidores y estaciones de trabajo.

Core.3 Linux Procedures.Machine Control.Files/Folder Control

- **Change File/Folder Permissions**
  - Lectura, escritura, ejecución 4 2 1
- **Change Group Ownership**
  - chgrp groupName folderName
- **Change Ownership**
  - chown userName fileFolderName
- **Delete any file or any folder - Dangerous**
  - Este procedimiento elimina cualquier archivo o carpeta sin solicitar permiso.

Core.3 Linux Procedures.Machine Control.Linux Kernel

- **Create an initrd image**
  - Crea una imagen initrd del sistema Linux y la nombra initrd.image-#versión# según el valor de versión introducido por usted.

Core.3 Linux Procedures.Machine Control.Monitoring

- **Get SNMP Conf file**
  - Recupera el archivo de configuración de SNMP con GETFILE.

Core.3 Linux Procedures.Machine Control.Networking

- **Setup DHCP Client**
  - Agrega entradas para que la interfaz obtenga información del servidor DHCP.
- **Setup Networking (1 interface)**
  - Crea un nuevo archivo de interfaces en /etc/networking con la información de la nueva dirección IP. Esto sólo configura la conexión a redes para una interfaz. Una vez que se crea el archivo, se reinicia el servicio de red.

Core.3 Linux Procedures.Machine Control.Networking.Get DOMAIN info

- **Query All Domain Information**
  - Lleva a cabo una búsqueda DNS completa de un nombre de dominio especificado mediante el comando DIG y el modificador ANY (búsqueda amplia, en toda la información de dominio). Luego, recupera el archivo de registro resultante, dig-#dominio#-all.log, y lo envía a la carpeta GetFile() del sistema.
- **Query DNS Server for Domain Details**
  - Lleva a cabo una búsqueda DNS de un nombre de dominio especificado mediante el comando DIG y recupera el archivo de registro resultante, dig-#dominio#-all.log, y lo envía a la carpeta GetFile() del sistema.
- **Query DNS Servers Authoritative for a Domain**
  - Lleva a cabo una búsqueda en el servidor de nombres autoritativo de un nombre de dominio especificado mediante el comando DIG y el modificador NS (servidores DNS autoritativos para el dominio). Luego, recupera el archivo de registro resultante, dig-#dominio#-Auth.log, y lo envía a la carpeta GetFile() del sistema.
- **Query Domain Address Records**
  - Lleva a cabo una búsqueda DNS de registros de dirección (A) de un nombre de dominio especificado mediante el comando DIG y el modificador NS (servidor DNS autoritativo para el dominio). Luego, recupera el archivo de registro resultante, dig-#dominio#-A.log, y lo envía a la carpeta GetFile() del sistema.
- **Query Domain Email Servers**
  - Lleva a cabo una búsqueda DNS de registros de servidores de correo electrónico y de agente de intercambio de correo (MX) de un nombre de dominio especificado mediante el comando DIG y el modificador MX (agentes de intercambio de correo para el dominio). Luego, recupera el archivo de registro resultante, dig-#dominio#-MX.log, y lo envía a la carpeta GetFile() del sistema.
- **Query Statistics Including Round-Trip Time**
  - Lleva a cabo una consulta DNS de estadísticas (incluido el tiempo de ida y vuelta) de un nombre de dominio especificado mediante el comando DIG y recupera el archivo de registro resultante, dig-#dominio#-stats.log, y lo envía a la carpeta GetFile() del sistema.
- **Query the TTL for Each Resource Record**
  - Lleva a cabo una consulta DNS de tiempo de vida (TTL) de un nombre de dominio especificado mediante el comando DIG y recupera el archivo de registro resultante, dig-#dominio#-TTL.log, y lo envía a la carpeta GetFile() del sistema.

Core.3 Linux Procedures.Machine Control.Networking.Routing

- **Get Routes**
  - Recupera la configuración de las rutas actuales.

- **Trace Path to Domain/IP**
  - Rastrea los saltos al dominio o a la dirección IP; usa GetFile para ver los resultados.

Core.3 Linux Procedures.Machine Control.Reboot/Shutdown

- **Reboot Linux**
  - Reinicia el sistema.
- **Shutdown Linux**
  - Cierra el sistema Linux.

Core.3 Linux Procedures.Machine Control.Runlevel Control

- **Custom Runlevel**
  - Consulte la explicación sobre niveles de ejecución en Linux en http://es.wikipedia.org/wiki/Nivel_de_ejecuci%C3%B3n.
- **Runlevel 1**
  - El nivel de ejecución 1 suele ser para comandos muy básicos. Es el equivalente al “modo seguro” de Windows. En general, sólo se utiliza para evaluar reparaciones o tareas de mantenimiento del sistema. Es un modo de usuario único y no permite que otros usuarios inicien sesión en la máquina.
- **Runlevel 2**
  - El nivel de ejecución 2 se utiliza para iniciar la mayoría de los servicios de la máquina. Sin embargo, no inicia el servicio de uso compartido de archivos de red (SBM, NFS). Permite que varios usuarios inicien sesión en la máquina.
- **Runlevel 3**
  - El nivel de ejecución 3 suele ser utilizado por los servidores. Carga todos los servicios, excepto el sistema de ventanas X. Esto significa que el sistema arranca de manera similar al DOS. Las GUI (KDE, Gnome) no se inician. Este nivel permite que varios usuarios inicien sesión en la máquina.
- **Runlevel 4**
  - En general, el nivel de ejecución 4 es personalizado. De manera predeterminada, inicia algunos servicios más que el nivel 3. Es un nivel que suele utilizarse sólo en circunstancias especiales.
- **Runlevel 5**
  - El nivel de ejecución 5 es el más completo. Inicia todas las GUI, los servicios adicionales de impresión y los servicios de terceros. Además, admite la modalidad multiusuario. Este nivel de ejecución suele utilizarse en las estaciones de trabajo.

Core.3 Linux Procedures.Machine Control.Services Control

- **Custom Services Control**
  - Inicia, detiene y reinicia cualquier servicio en el sistema.
- **Restart HTTPD/Apache2**
  - Reinicia el servicio web HTTPD/Apache2.
- **Restart Networking**
  - Reinicia el demonio de conexión a redes.
- **Restart NFS**
  - Reinicia los demonios de servicios NFS.
- **Restart Postfix**
  - Reinicia un servidor de correo electrónico Postfix.
- **Restart SSH**
  - Reinicia el servidor SSH.

- **Restart VMWare Tools**
  - Reinicia VMWare Tools.

Core.3 Linux Procedures.Machine Control.User/Group Control.Groups

- **Create new group**
  - Usa GROUPADD para crear un grupo nuevo especificado.
- **Delete Group**
  - Usa GROUPDEL para eliminar un grupo existente especificado.

Core.3 Linux Procedures.Machine Control.User/Group Control.Password Control

- **Change Root Password**
  - Cambia la contraseña raíz del sistema. Por algún motivo, el script devuelve el estado FAILED (Erróneo), pero aun así funciona :).
- **Change user password**
  - Solicita el nombre de usuario y restablece la contraseña.

Core.3 Linux Procedures.Machine Control.User/Group Control.Users

- **Add New User**
  - Agrega un nuevo usuario de Linux.
- **Eliminar Usuario**
  - Elimina un usuario del servidor o de la máquina.

Core.3 Linux Procedures.Machine Control.Utils

- **Add custom commands**
  - Agrega algunos comandos personalizados con alias al archivo /root/.bashrc y luego lo ejecuta para que dichos comandos se lleven a cabo. Los comandos personalizados son los siguientes:

    ll = ls –l
    la = ls -A
    l = ls -CF
    *** Extend by adding more aliased commands ***
- **Synchronize the System Clock**
  - Instala y sincroniza el reloj del sistema.
- **Update File Database**
  - Actualiza la base de datos del sistema de archivos para utilizar el comando “locate”.

Core.3 Linux Procedures.Maintenance

- **Collect inode usage statistics**
  - Revisa el uso de los inodos.
- **Force Logical File System Check (FSCK) at Next Reboot**
  - Fuerza la ejecución de una comprobación del sistema de archivos (FSCK) durante el próximo reinicio.
- **Get Disk Usage**
  - Genera un listado de uso del disco mediante DF, escribe los resultados en el registro de procedimientos de agente, los recupera y los envía a la carpeta GetFile() del sistema.
- **Linux Weekly Maintenance**
  - Lleva a cabo varias tareas de mantenimiento de rutina en equipos Linux, entre las que se incluyen sincronización de la hora, limpieza del repositorio apt-get, actualizaciones de paquetes, comprobaciones de disco y estadísticas de rendimiento.

- **Remove User Adobe Flash/Macromedia Permanent Objects**
  - Elimina los objetos permanentes de Adobe Flash y Macromedia del usuario.
- **Remove User Temporary Files**
  - Elimina los archivos temporales (es decir, *~) de la carpeta particular del usuario actual.

Core.3 Linux Procedures.Process Control.Get All Processes with PID

- Recupera todos los procesos con ID de proceso; utiliza la característica GETFILE para recuperar los resultados.

- **Get process Tree**
  - Genera un árbol de procesos primarios y secundarios; utiliza la característica GETFILE para recuperar los resultados.
- **Kill Process**
  - Se usa la variable con el PID correcto para eliminar el proceso especificado.
- **Locate a file**
  - Usa la función “locate” de Kaseya para buscar los archivos especificados; utiliza la característica GETFILE para recuperar los resultados.

Core.3 Linux Procedures.Setup/Configs.Backup Servers

- **MySQL Backups With AutoMySQLBackup On Ubuntu 9.10**
  - Se requiere la instalación de Postfix antes de instalar AutoMySQLBackup. Se requiere Postfix (http://sourceforge.net/projects/automysqlbackup/, http://www.mysql.com/).
- **Ubuntu Server 9.04 Bacula Bweb GUI**
  - No probado.

Core.3 Linux Procedures.Setup/Configs.CRM Servers.SugarCRM

- Se requiere la instalación completa del servidor LAMP antes de instalar SugarCRM (MySQL, Apached, PHP). Una vez finalizado el script, ejecute lo siguiente: http://Server IP Address/sugarcrm

Core.3 Linux Procedures.Setup/Configs.DNS

- **Setup Chrooted DNS Server**
  - Configura la ejecución de BIND en un entorno chroot.

Core.3 Linux Procedures.Setup/Configs.Email Server

- **(2) Configure Postix Email Server**
  - Configura el servidor de correo electrónico Postfix.
- **(2.1) Configure SMTP-AUTH**
  - Configura la autenticación SMTP segura mediante SASLAUTHD.
- **(3) Create the certificates for TLS**
  - Genera certificados TLS.
- **(4) Configure Postfix for TLS**
  - Configura las claves seguras de TLS para utilizar Postfix.
- **(5) Configure SASLAUTHD to work with Chrooted Postfix**
  - La autenticación se realiza mediante SASLAUTHD. Es necesario modificar algunas cosas para que funcione correctamente. Dado que Postfix se ejecuta en forma chroot en /var/spool/postfix, es necesario hacer lo siguiente:
- **(6) Install Courier-IMAP/Courier-POP3**
  - Instala y configura los servicios IMAP y POP3 con Courier y modifica los dos archivos siguientes. Reemplace CN=localhost por CN=server1.example.com (también es posible

modificar los otros valores, si fuera necesario): vim /etc/courier/imapd.cnf vim /etc/courier/pop3d.cnf

- **(7) Configure Maildir**
  - Configura Maildir para los mensajes de correo electrónico y los buzones de correo de los usuarios.

Core.3 Linux Procedures.Setup/Configs.FTP Servers

- **Configure Proftpd**
  - Configura el servidor Proftpd. Recuerde instalar el software previamente.

Core.3 Linux Procedures.Setup/Configs.MySQL Server

- **MySQL Server Installation**
  - Instala MySQL Server y establece la contraseña raíz.

Core.3 Linux Procedures.Setup/Configs.NFS.NFS Client

- **Install and config for NFS Client**
  - Configura NFS para que las máquinas cliente monten las unidades exportadas o compartidas por el servidor.

Core.3 Linux Procedures.Setup/Configs.NFS.NFS Server

- **Install and Setup NFS Server**
  - Instala y configura el servidor NFS con el directorio HOME y un directorio opcional compartido con las máquinas cliente.

Core.3 Linux Procedures.Setup/Configs.Security.AppArmor

- **Disable AppArmor**
  - AppArmor es una extensión de seguridad (similar a SELinux) que debería proporcionar mayor seguridad. Creemos que no es necesaria para configurar un sistema seguro. En general, los problemas que genera son mayores que las ventajas que brinda (imagine una semana de llevar a cabo tareas para solucionar problemas porque uno de los servicios no funciona como se esperaba y detectar luego que todo estaba en orden, y que AppArmor que era la causa del problema). Por lo tanto, se sugiere deshabilitarlo.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Forward Rules

- **Deny Access to a Specific Subnet**
  - Deniega el acceso a una subred especificada mediante la adición de reglas de firewall de iptables adecuadas.
- **Forward Traffic (DNAT)**
  - Permite el reenvío DNAT de un puerto TCP determinado al servidor interno. Debe especificar la interfaz pública, la dirección pública, la dirección del servidor interno y el puerto; el procedimiento agrega las reglas de firewall de iptables adecuadas.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Global Rules (REJECT, ACCEPT)

- **# Forwarding Traffic (DROP ALL)**
  - Rechaza todo el tráfico de la cadena de reenvío.
- **# Incoming Traffic (ALLOW ALL)**
  - Permite todo el tráfico entrante mediante la cadena INPUT.
- **# Incoming Traffic (DROP ALL)**
  - Rechaza todo el tráfico entrante.
- **# Outgoing Traffic (ALLOW ALL)**

  - Permite todo el tráfico saliente desde su red interna.
- **# Outgoing Traffic (DROP ALL)**
  - Rechaza la salida del tráfico de la red interna por el firewall.
- **_### NB! - Enable Routing - NB! ###_**
  - Habilita el enrutamiento y NAT para iptables; es importante para que el tráfico se procese a través del firewall.
- **Don't Accept ICMP Redirect Messages**
  - Configura el sistema de manera que no acepte redirecciones ICMP.
- **Don't Send ICMP Redirect Messages**
  - Configura el sistema de manera que no envíe redirecciones ICMP.
- **Drop ICMP echo-request Messages Sent to Broadcast or Multicast Addresses**
  - Configura el sistema de manera que descarte los mensajes de solicitud de eco ICMP enviados a direcciones de difusión y multidifusión.
- **Drop Source Routed Packets**
  - Configura el sistema de manera que descarte los paquetes enrutados de origen.
- **Enable Logging**
  - Habilita el registro de eventos del firewall de iptables.
- **Enable Source Address Spoofing Protection**
  - Habilita la protección contra la suplantación de direcciones de origen en el sistema.
- **Enable TCP SYN cookie protection from SYN floods**
  - Habilita la protección de cookies TCP SYN contra las inundaciones SYN en el sistema.
- **Flush All Chains**
  - Vacía todas las reglas de iptables. Esto es peligroso. Úselo bajo su responsabilidad.
- **Log Packets with Impossible Source Addresses**
  - Habilita el registro de paquetes con direcciones de origen imposibles en el sistema.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Inbound Rules

- **Allow CUSTOM Port Inbound**
  - Permite introducir una interfaz, un protocolo y un puerto TCP/UDP para agregar a las reglas de firewall de iptables.
- **Allow DNS Inbound**
  - Permite el tráfico entrante de DNS por medio de la adición de las reglas de firewall de iptables adecuadas. No se aplica solamente a los firewalls que funcionan como clientes DNS, sino también a aquellos que funcionan con un rol de servidor DNS regular o de almacenamiento en caché.
- **Allow FTP Inbound**
  - Permite el tráfico entrante de FTP por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow ICMP Inbound**
  - Permite el tráfico entrante de ICMP por medio de la adición de las reglas de firewall de iptables adecuadas. iptables se configura de manera que permita al firewall enviar solicitudes de eco ICMP (pings) y, a la vez, aceptar las respuestas de eco ICMP esperadas.
- **Allow IMAP Inbound**
  - Permite el tráfico entrante de IMAP por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow IMAPS Inbound**

- Permite el tráfico entrante de IMAPS por medio de la adición de las reglas de firewall de iptables adecuadas.

- **Allow Kaseya Inbound**
  - Permite el tráfico entrante de Kaseya por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow Loopback interface**
  - Permite el tráfico entrante de la interfaz de bucle invertido por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow MySQL**
  - Permite el tráfico entrante de MySQL por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow Network to Access Firewall**
  - eth1 está conectado directamente a una red privada mediante direcciones IP de la red 192.168.1.0. De manera simplista, se presupone que todo el tráfico entre esta red y el firewall es confiable y está permitido. Se necesitan más reglas para que la interfaz conectada a Internet permita que sólo determinados puertos, tipos de conexiones y, posiblemente, incluso servidores remotos, tengan acceso a su firewall y su red doméstica.
- **Allow POP3 Inbound**
  - Permite el tráfico entrante de POP3 por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow POP3S Inbound**
  - Permite el tráfico entrante de POP3S por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow SMTP Inbound**
  - Permite el tráfico entrante de SMTP por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow SSH Inbound**
  - Permite el tráfico entrante de SSH por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow Traffic from Localhost**
  - Permite el tráfico entrante de la dirección de localhost por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow WWW Inbound**
  - Se permiten los paquetes entrantes destinados a los puertos 80 y 22. De esa manera, se comienza a establecer la conexión. No es necesario especificar estos puertos para el tramo de regreso dado que se permiten los paquetes salientes para todas las conexiones establecidas. Las conexiones iniciadas por personas conectadas al servidor web se deniegan, dado que no se permiten NUEVOS paquetes de conexión salientes.
- **Allow Established Sessions Inbound**
  - Permite el tráfico entrante de las sesiones establecidas por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Block IP Address**
  - Bloquea el acceso de una dirección IP especificada a su red por medio de la interfaz pública.
- **Block IRC Inbound**
  - Bloquea el tráfico entrante de IRC por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Block Network**
  - Bloquea el acceso de una red completa a su red.

- **List all iptables Rules**
  - Canaliza todas las reglas de iptables en /var/tmp/iptables.log, el cual, por medio del procedimiento GET, se carga al servidor para su revisión.
- **Restart IPTables**
  - Reinicia el firewall iptables.
- **Save iptables Rules**
  - Probado en Ubuntu.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Outbound Rules

- **# Allow Kaseya Outbound**
  - Permite el tráfico saliente de Kaseya por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow CUSTOM Port Outbound**
  - Permite que un puerto personalizado de su red interna tenga acceso al exterior.
- **Allow DNS Outbound**
  - Las siguientes instrucciones no se aplican solamente a los firewalls que funcionan como clientes DNS, sino también a aquellos que funcionan con un rol de servidor DNS regular o de almacenamiento en caché.
- **Allow Established Connections Outbound**
  - Permite todas las conexiones establecidas con ACK.
- **Allow FTP Outbound**
  - Permite el tráfico saliente de FTP por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow ICMP Packets Outbound**
  - Permite el tráfico saliente de los paquetes ICMP por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow IMAP Outbound**
  - Permite el tráfico saliente de IMAP por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow IMAPS Outbound**
  - Permite el tráfico saliente de IMAPS por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow Loopback Interface**
  - Permite el tráfico saliente de la interfaz de bucle invertido por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow MySQL Outbound**
  - Permite el tráfico saliente de MySQL por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow POP3 Outbound**
  - Permite el tráfico saliente de POP3 por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow POP3S Outbound**
  - Permite el tráfico saliente de POP3S por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow SMTP Outbound**
  - Permite el tráfico saliente de SMTP por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow SSH**

  - Permite el tráfico saliente de SSH por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Allow WWW**
  - Permite el tráfico saliente de WWW por medio de la adición de las reglas de firewall de iptables adecuadas.
- **Deny Access to a Specific Outbound IP Address with Logging**
  - Deniega el acceso (con registro) a una dirección IP saliente especificada mediante la adición de reglas de firewall de iptables adecuadas.
- **FLUSH OUTBOUND Rules**
  - Vacía las reglas de salida de iptables. Esto es peligroso. Úselo bajo su responsabilidad.
- **Run all OUTBOUND Rules**
  - Aplica todas las reglas de salida con la posibilidad de vaciar opcionalmente todas esas reglas primero.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Postrouting Rules

- **Allow routing for private network through Firewall**
  - Observará que la red privada es una red IP enrutada no pública. Esto requiere la traducción de direcciones por parte de un enrutador con una dirección IP pública. De lo contrario, desde la red pública no se podrán devolver paquetes a la red privada. La traducción de direcciones se habilita fácilmente con iptables. Las direcciones que se traducen son el "origen" de las sesiones, por lo que el modo se denomina Source NAT (SNAT):

Core.3 Linux Procedures.Setup/Configs.Security.SELinux

- **Disable SELinux after reboot**
  - Deshabilita SELinux de manera permanente después del primer reinicio.
- **Disable SELinux Immediately**
  - Deshabilita SELinux en el nivel de ejecución actualmente conectado. Este no se configura para deshabilitarse después del reinicio.

Core.3 Linux Procedures.Setup/Configs.Shell Control

- **Change The Default Shell**
  - /bin/sh en un enlace simbólico a /bin/dash. Sin embargo, es necesario /bin/bash, no /bin/dash.

Core.3 Linux Procedures.Setup/Configs.Web Servers.Apache2

- **Enable Modules**
  - Módulos de Apache (SSL, rewrite, suexec, include y WebDAV):
- **Install Apache2**
  - Usa APT-GET para instalar el servidor web Apache2, usa CHKCONFIG para establecer el inicio automático e inicia el demonio de Apache.
- **Install PHPMyAdmin**
  - Asegúrese de modificar la configuración de Apache para que phpMyAdmin permita otras conexiones además de las de localhost (mediante la conversión en comentario de la estrofa <Directory /usr/share/phpMyAdmin/>):

Core.3 Linux Procedures.Setup/Configs.Web Servers.Scripting

- **Install PHP5**
  - Instala PHP5 para Apache 2.

Core.3 Linux Procedures.Software Control.Applications

- **Install CHKCONFIG**
  - Instala el paquete CHKCONFIG. Este paquete permite iniciar un paquete de demonio determinado al arrancar el sistema.
- **Install CHKCONFIG Simple**
  - Usa APT-GET para instalar CHKCONFIG.
- **Install Common needed packages**
  - Instala paquetes comúnmente necesarios para Ubuntu. binutils cpp fetchmail flex gcc libarchive-zip-perl libc6-dev libcompress-zlib-perl libdb4.6-dev libpcre3 libpopt-dev lynx m4 make ncftp nmap openssl perl perl-modules unzip zip zlib1g-dev autoconf automake1.9 libtool bison autotools-dev g++ build-essential
- **install SNMP**
  - Instala SNMP, el cual permite supervisar los servidores Linux. Recuerde establecer la cadena de comunidad SNMP.
- **Instalar Software**
  - Solicita al usuario el nombre del paquete de software que es necesario instalar y, luego, lo instala por medio de APT-GET.
- **Install software from Image List**
  - Permite separar con barras verticales (|) una lista de software para el comando apt-get install, el cual instala el software faltante de la lista. Primero se debe crear la lista. NB (consulte la carpeta de actualizaciones de software para obtener información sobre el procedimiento de creación de la lista de imágenes.
- **Install SSH**
  - Instala el servidor SSH para acceso remoto.
- **Install VIM**
  - Instala VIM, un editor de archivos de texto para Linux fácil de usar.
- **Install vim-nox**
  - El programa vi predeterminado tiene un comportamiento extraño en Ubuntu y Debian. Para corregir este problema, se instala vim-nox:
- **Install XPDF**
  - Lector de PDF para Linux.

Core.3 Linux Procedures.Software Control.apt-get

- **Autoclean apt-get**
  - El comando apt-get autoclean sólo quita los archivos de paquete que ya no pueden descargarse.
- **Clean apt-get repository**
  - Elimina todo, excepto los archivos bloqueados, de /var/cache/apt/archives/ y /var/cache/apt/archives/partial/. Por lo tanto, si necesita reinstalar un paquete, APT debe recuperarlo otra vez.
- **Instalar Software**
  - Solicita al usuario el nombre del paquete de software que es necesario instalar y, luego, lo instala por medio de APT-GET.
- **Remove Software**
  - Elimina el paquete solicitado por el procedimiento.

Core.3 Linux Procedures.Software Control.DNS

- **Install Bind9**

- Servidor DNS para Linux.

Core.3 Linux Procedures.Software Control.Email Servers

- **Download Zimbra Email**
  - Descarga el paquete de aplicaciones de colaboración y correo electrónico Zimbra para Linux.

Core.3 Linux Procedures.Software Control.File Server

- **Install Quota**
  - Instala la aplicación necesaria para el control de cuotas en las carpetas determinadas. Se recomienda especialmente editar su archivo /etc/fstab de forma manual ya que puede dañar su servidor y no montar ningún sistema de archivos. A continuación, se presenta un ejemplo de un archivo fstab con cuotas habilitadas que funciona correctamente:

```
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    nodev,noexec,nosuid 0       0
/dev/mapper/server1-root /              ext4
errors=remount-ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0
1
# /boot was on /dev/sda1 during installation
UUID=a8f37dcf-5836-485c-a451-3ae2f0f47720 /boot          ext2    defaults
0       2
/dev/mapper/server1-swap_1 none           swap    sw            0       0
/dev/fd0        /media/floppy0  auto    rw,user,noauto,exec,utf8 0       0
```

- **Set Quota on**
  - Habilita la administración de cuotas para servidores de archivos.

Core.3 Linux Procedures.Software Control.FTP Servers

- **Install Proftpd**
  - Instala el servidor Proftpd para Linux.

Core.3 Linux Procedures.Software Control.iptables (Firewall)

- **Install iptables**
  - Usa APT-GET para instalar un firewall iptables.

Core.3 Linux Procedures.Software Control.Management Software

- **Download Webmin**
  - Webmin es una GUI útil para la administración completa de Linux mediante un explorador web.

Core.3 Linux Procedures.Software Control.Repository's

- **Enable Multiverse Repository**
  - Agrega los orígenes al archivo source.list. No se vuelve a crear el archivo.
- **Enable Universe Repository**
  - Este procedimiento agrega el contenido de este repositorio al archivo de orígenes. No se vuelve a crear el archivo.
- **Update Repository's**
  - Actualiza todos los paquetes. Ejecútelo después de agregar el contenido del repositorio.

Core.3 Linux Procedures.Software Control.System

- **Install NTP Daemon**
  - Es recomendable sincronizar el reloj del sistema con un servidor NTP (protocolo de tiempo de redes) en Internet. Simplemente, ejecútelo.

Core.3 Linux Procedures.Software Control.Updates/Upgrades

- **Create Image List of Installed Software**
  - Crea una lista de imágenes del software instalado.
- **Full System Update**
  - Actualiza todos los paquetes del sistema.
- **Upgrade Packages**
  - Use este procedimiento para actualizar los paquetes de una misma distribución.
- **Upgrade to New Release**
  - Actualiza la distribución de Linux a la versión más reciente disponible. Al terminar, verá una solicitud de reinicio en el escritorio.
- **Linux Package Updates/Upgrades**
  - Lleva a cabo una actualización completa del sistema y de todos los paquetes instalados.

Core.4 Other Tools and Utility Procedures

Core.4 Other Tools and Utility Procedures.AntiVirus

- **EICAR Virus Test**
  - Crea un archivo en el directorio de trabajo de agente que contiene el patrón de virus de prueba EICAR. Este procedimiento de agente se puede utilizar para verificar que cualquier software antivirus en una máquina está en funcionamiento. NOTA: No se trata de un virus real y no conlleva ningún riesgo. Para obtener más información, consulte http://eicar.org.
- **Run a Malicious Software Removal Tool Full Scan-Clean**
  - Usa MRT (la herramienta de eliminación de software malintencionado de Microsoft) para realizar un análisis y una limpieza completos. Los resultados de la operación se registran en un archivo MRT.LOG y en el registro de procedimientos de agente. El archivo de registro se recupera y se envía a la carpeta GetFile() del sistema.

Core.4 Other Tools and Utility Procedures.AntiVirus.Defender

- **Windows Defender - Full System Scan**
  - Ejecuta un análisis completo del sistema con Windows Defender.
- **Windows Defender - Quick System Scan**
  - Ejecuta un análisis rápido del sistema con Windows Defender.
- **Windows Defender - Signature Update**
  - Ejecuta una actualización de firmas con Windows Defender.

Core.4 Other Tools and Utility Procedures.AutoAdminLogon

- **Disable AutoAdminLogon**
  - Deshabilita toda configuración de AutoAdminLogon previamente habilitada en un equipo Windows.
- **Enable AutoAdminLogon with AUTOLOGON**
  - Habilita AutoAdminLogon con cifrado de contraseña segura mediante la utilidad AutoLogon de SysInternals. Este procedimiento de agente sólo funciona en versiones de 32 bits de Windows XP o posterior.
- **Enable AutoAdminLogon with Cleat Text Method**
  - Solicita el nombre de usuario y la contraseña para AutoAdminLogin y, luego, habilita la configuración de AutoAdminLogin con texto no cifrado en un equipo Windows mediante las credenciales proporcionadas.

Core.4 Other Tools and Utility Procedures.Kaseya Agent Management

- **Agent - Force Check-in**
  - Este es el procedimiento más corto del mundo. No tiene ningún paso. Su único trabajo es forzar al agente a conectarse al KServer. Usar Forzar Conexión para determinar si el agente está en línea o no.
- **Agent - Remove Kaseya from Start Menu and Add-Remove Programs**
  - Quitar la carpeta del Agente desde el Menú Inicio. Ocultar el Icono de Bandeja del Sistema (K azul) deshabilitando el Menú Agente (pestaña Agente - Menú Agente). Ejecutar este script en máquinas en las que no desee darle a nadie la habilidad de desinstalar, salir o detener el Agente.
- **Agent - Reset Audit Cache**
  - Elimina el archivo de resultados de auditoría en caché guardado por el agente. Ejecutar este procedimiento para resetear todos los resultados de aplicaciones de una auditoría y volver a iniciar.
- **Agent - Terminate Remote Control Sessions**
  - Este script finaliza todas las sesiones de control remoto que Kaseya admite en la función de control remoto del VSA (K-VNC, WinVNC, Terminal Services, FTP, RAdmin y pcAnyWhere).
- **VNC - Hide System Tray Icon**
  - Deshabilita el ícono de bandeja del sistema de VNC en los equipos Windows cuando el servicio VNC está en ejecución.
- **VNC - Set Idle Timeout to 0 (Never Timeout)**
  - Establece el tiempo de espera de inactividad del VNC en 0 para que una sesión inactiva de control remoto del VNC no se desconecte. Resulta de utilidad al llevar a cabo operaciones remotas que tardan mucho tiempo en completarse en máquinas y cuando no se desea que se agote el tiempo de espera de la sesión del VNC automáticamente después de 1 hora de inactividad (valor predeterminado).
- **VNC - Habilitar fondo de escritorio cuando se maneja remotamente**
  - Habilita el papel tapiz cuando se controla un sistema de manera remota y, a la vez, deshabilita el ícono de VNC para un control remoto totalmente silencio del agente.
- **VNC - Remove RealVNC from Start Menu**
  - Quita la entrada de RealVNC del menú Inicio.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Ping Check

- **Ping IP Dirección 1**
  - Este procedimiento ejecuta un ping en la dirección IP para obtener resultados que usted pueda usar en otro procedimiento. Esto también podría ser un puerto o cualquier otro dispositivo.
- **Ping IP Dirección 2**
  - Este procedimiento probará la variable desde las Direcciones de IP de Ping para ver si puede enviar un ping a la dirección sin pérdida de paquete. Si hay pérdida de paquete, el sistema envía un correo electrónico con los resultados del ping. Si no hay pérdida de paquete, se registra en el resultado Todo OK.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Port Check

- **Monitor de Puerto 1**
  - Parte 1 de 2: Monitorear un puerto en un host o dirección de IP y enviar un correo electrónico cuando el puerto no responde. Editar el paso 1 con el nombre de host o dirección de IP, Editar el paso 2 para ingresar el número de puerto que desea monitorear y editar el paso 3 para especificar las direcciones de correo electrónico (múltiples direcciones

separadas por coma) para enviar una alerta cuando el puerto no responda. Editar el procedimiento Port Monitor 2 para modificar el asunto y cuerpo del correo electrónico.

- **Monitor de Puerto 2**
  - NO programar este procedimiento. Este es un procedimiento secundario llamado por Port Monitor 1. Programar Port Monitor 1 para que se ejecute en una máquina para monitorear un puerto en un host o Dirección de IP.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Web Check

- **Comprobar Web 1**
  - Este procedimiento extrae el resultado de la página web configurada como la variable siteURL. El script Check Web 2 verifica que el resultado tenga el contenido esperado. Debe configurar la variable siteURL y la cadena de búsqueda del archivo de prueba en Check Web 2 para personalizar el procedimiento. En este ejemplo, se busca la palabra “google” en www.google.com/index.html.
- **Comprobar Web 2**
  - El script Check Web 2 verifica que el resultado obtenido de la solicitud de URL tenga el contenido esperado. Debe modificar el comando del archivo de prueba para que refleje el contenido que se debe encontrar en la URL de prueba. En este ejemplo, se busca la palabra “google” en la página principal de Google.

Core.4 Other Tools and Utility Procedures.Managed Services.Policy Management

- **Windows Group Policy Update (GPUPDATE /FORCE)**
  - Vuelve a cargar la directiva de grupo en los equipos Windows.

Core.4 Other Tools and Utility Procedures.Managed Services.Server Management.Services Remediation

- **Iniciar Servicio (W32Time)**
  - Este procedimiento reinicia el servicio de hora de Windows. Este es un procedimiento de ejemplo en el que se demuestra de qué manera iniciar un servicio con los procedimientos de agente de Kaseya.
- **Detener Servicio (W32Time)**
  - Este procedimiento detiene el servicio de hora de Windows. Este es un procedimiento de ejemplo en el que se demuestra de qué manera detener un servicio con los procedimientos de agente de Kaseya.

Core.4 Other Tools and Utility Procedures.Managed Services.Server Management.Terminal Services

- **Change Terminal Services RDP Listening Port**
  - Este procedimiento cambia el puerto RDP predeterminado para Terminal Services de 3389 a un nuevo puerto que elija.

Core.4 Other Tools and Utility Procedures.Managed Services.System Management

- **Descargar SysInternals Process Explorer**
  - En este ejemplo, se demuestra de qué manera descargar archivos de orígenes remotos mediante el comando de procedimiento de agente Get URL. Simplemente especifique la URL para la descarga y la ubicación de destino. En este ejemplo, se realiza la descarga directamente de la página web del proveedor. Sin embargo, un método muy utilizado para distribuir archivos es almacenarlos en un FTP o una página web de acceso público (almacenamiento en la nube) y utilizar este método para descargarlos en los extremos. En este ejemplo sólo se descarga un archivo. Sin embargo, es posible ampliar la funcionalidad para instalar o ejecutar archivos con el comando execute shell en los procedimientos de agente. También tenga en cuenta que en este script se usa una variable para el directorio

temporal del agente. Consulte **Ruta de acceso del directorio de trabajo de agente** en **Uso de variables** *(http://help.kaseya.com/webhelp/ES/VSA/R8/index.asp#2855.htm)* en la ayuda en línea del VSA.

- **Enviar mensaje si está conectado**
  - Esto envía un mensaje a todos sus usuarios si necesita realizar mantenimiento. En un sistema, puede usar la pestaña de control remoto para enviar un mensaje, pero no hay manera de enviar un mensaje si están conectados.

Core.4 Other Tools and Utility Procedures.Operational Communications

- **Copy OpComm Messages**
  - Copia los últimos archivos de mensaje de OpComm del servidor a la máquina de destino.
- **Get User name - Then Welcome**
  - Recupera el usuario actualmente conectado de una vista SQL y envía el mensaje “Welcome to our IT Support service” (Bienvenido a nuestro servicio de soporte de TI)" a ese usuario. En caso de que no haya un usuario conectado, el procedimiento de agente se vuelve a programar para ejecutarse a los 10 minutos.
- **OpComm-ActionRequired**
  - Muestra el mensaje de OpComm ActionRequired (Acción requerida) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-Backup**
  - Muestra el mensaje de OpComm Backup (Copia de seguridad) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-Emergency**
  - Muestra el mensaje de OpComm Emergency (Emergencia) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-MachineAudit**
  - Muestra el mensaje de OpComm MachineAudit (Auditoría de máquina) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-MaintSchedule**
  - Muestra el mensaje de OpComm MaintSchedule (Programación de mantenimiento) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-NetworkDowntime**

- Muestra el mensaje de OpComm NetworkDowntime (Tiempo de inactividad de la red) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.

- **OpComm-PatchUpdate**
  - Muestra el mensaje de OpComm PatchUpdate (Actualización de parches) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-RegularMaintenance**
  - Muestra el mensaje de OpComm RegularMaintenance (Mantenimiento regular) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-VirusScan**
  - Muestra el mensaje de OpComm VirusScan (Análisis de virus) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-VirusThreat**
  - Muestra el mensaje de OpComm VirusThreat (Amenaza de virus) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.
- **OpComm-Welcome**
  - Muestra el mensaje de OpComm Welcome (Bienvenido) al usuario conectado. Los mensajes de OpComm sirven para comunicar actividades operativas, notificaciones y recordatorios estándar. La carpeta de mensajes de OpComm se puede personalizar y ampliar a fin de admitir otros tipos de comunicaciones de usuarios finales. Estos archivos se encuentran en la carpeta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm en Kaseya Server.

Core.4 Other Tools and Utility Procedures.Patch Management

- **WinAutoUpdate Status Check**
  - Comprueba el último estado conocido de la actualización automática de Windows de acuerdo con la detección de parches más reciente y ejecuta “WinAutoUpdate Enabled” si está habilitada o “WinAutoUpdate Disabled” si está deshabilitada. Se usa para crear Vistas que muestren las máquinas en las cuales la actualización automática de Windows está habilitada o deshabilitada.
- **WinAutoUpdate Disabled**

- NO EJECUTAR O PROGRAMAR ESTE PROCEDIMIENTO. Es invocado por "WinAutoUpdate Status Check" si la actualización automática de Windows está deshabilitada en una máquina.

- **WinAutoUpdate Enabled**
  - NO EJECUTAR O PROGRAMAR ESTE PROCEDIMIENTO. Es invocado por "WinAutoUpdate Status Check" si la actualización automática de Windows está habilitada en una máquina.
- **Create Repository Share**
  - Crea una carpeta local de origen de archivo y un recurso compartido de red para que funcionen como repositorio de los parches de Windows descargados de Internet mediante la administración de parches.
- **Patch Pre-Warning**
  - Envía un mensaje al usuario conectado para informarle que están por instalarse las actualizaciones de parches y de seguridad en la máquina. Está diseñado para usarse como procedimiento previo a las actualizaciones automáticas de parches.
- **Reinicio de Parche**
  - En las estaciones de trabajo Windows, el procedimiento solicita al usuario conectado que reinicie la máquina debido a la instalación de actualizaciones de parches y de seguridad. Si el usuario responde que sí, se le informa que el sistema se reiniciará en un minuto por lo que debe guardar su trabajo y cerrar las aplicaciones. Si el usuario responder que no, se programa para ejecutarse otra vez en 60 minutos. En caso de que no haya un usuario conectado a la estación de trabajo, el sistema se reinicia. Si la máquina es un servidor, y hay una dirección de correo electrónico de reinicio por instalación de parches configurada, el procedimiento envía un correo a dicha dirección en el cual indica que la máquina necesita atención (debe reiniciarse).

Core.4 Other Tools and Utility Procedures.Patch Management.Suspend Alarms After Patch

- **Patch Post-Unsuspend Alarms**
  - Reanuda las alarmas relacionadas con la supervisión. Está diseñado para usarse como procedimiento posterior a las actualizaciones automáticas de parches cuando la máquina se reinicia inmediatamente después de la aplicación de parches.
- **Suspend Alarms for 10mins**
  - Suspende las alarmas relacionadas con la supervisión por 10 minutos. Está diseñado para ejecutarse como procedimiento posterior a las actualizaciones automáticas de parches cuando se produce un reinicio automáticamente después de la aplicación de parches.
- **Suspend Alarms for 10mins - Recurring**
  - Suspende las alarmas relacionadas con la supervisión por 10 minutos y luego se vuelve a programar para ejecutarse en 5 minutos. De esa manera, se evitan posibles brechas durante el intervalo en que la alarma está suspendida. Está diseñado para ejecutarse como procedimiento posterior a las actualizaciones automáticas de parches cuando es posible que la máquina no se reinicie inmediatamente.
- **Suspend Alarms for 120mins**
  - Suspende las alarmas relacionadas con la supervisión por 120 minutos. Está diseñado para ejecutarse como procedimiento posterior a las actualizaciones automáticas de parches cuando no se produce un reinicio automáticamente después de la aplicación de parches.

Core.4 Other Tools and Utility Procedures.Run Now System Scripts

- **Run Now Baseline Audit**
  - Ejecuta el procedimiento de agente del sistema llamado "Auditoría de base".
- **Run Now Disable Windows Automatic Update**

  - Ejecuta el procedimiento de agente del sistema llamado “Deshabilitar actualización automática de Windows”.
- **Run Now Latest Audit**
  - Ejecuta el procedimiento de agente del sistema llamado “Última auditoría”.
- **Run Now Patch Scan**
  - Ejecuta el procedimiento de agente del sistema llamado “Detección de parches”.
- **Run Now Server Roles Audit**
  - Ejecuta el script de sistema LUA del lado cliente para llevar a cabo una auditoría de roles del servidor.
- **Run Now System Info**
  - Ejecuta el procedimiento de agente del sistema llamado “Información del sistema”.
- **Run Now Update Lists By Scan**
  - Ejecuta el procedimiento de agente del sistema llamado “Actualizar listas mediante análisis”.
- **Run Now Uninstall Agent (Retains Agent Data)**
  - Ejecuta el procedimiento de agente del sistema llamado “Desinstalar agente”. Después de la desinstalación del agente, el sistema conserva sus datos hasta que se eliminen de forma manual.
- **Run Now Reset Windows Automatic Update**
  - Ejecuta el procedimiento de agente del sistema llamado “Restablecer actualización automática de Windows”.

Conjuntos de Monitores

Respaldo

- **Backup - Backup Exec Continuous Protection Services - {Severity3}**
  - Supervisa los servicios de protección continua de Backup Exec en los servidores Backup Exec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Backup - Backup Exec DLO Agent Services - {Severity3}**
  - Supervisa los servicios de agentes DLO de Backup Exec en los servidores Backup Exec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Backup - Backup Exec Services - {Severity3}**
  - Supervisa los servicios de Backup Exec en los servidores Backup Exec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Backup - Backup Exec System Recovery Service - {Severity3}**
  - Supervisa los servicios de recuperación del sistema de Backup Exec en los servidores Backup Exec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Backup - BrightStor ARCServe Backup Services - {Severity3}**
  - Supervisa los servicios de BrightStor ARCServe Backup en los servidores BrightStor ARCServe Backup. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Base de datos

- **Database - SQL Server (All Instances) Services - {Severity3}**

- Supervisa los servicios de SQL Server en los servidores SQL Server que usan el servicio de comodines MSSQL*. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

- **Database - SQL Server (Default Instance) - {Severity0}**
  - Recolecta contadores de rendimiento de SQL Server (instancia predeterminada) en los servidores SQL Server. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Database - SQL Server (Default Instance) Performance - {Severity2}**
  - Supervisa el rendimiento de SQL Server (instancia predeterminada) en los servidores SQL Server. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Database - SQL Server (Default Instance) Services - {Severity3}**
  - Supervisa los servicios de SQL Server (instancia predeterminada) en los servidores SQL Server. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Database - SQL Server 2005 Optional Services - {Severity3}**
  - Supervisa los servicios opcionales de SQL Server 2005 en los servidores SQL Server 2005. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Database - SQL Server 2005 Services - {Severity3}**
  - Supervisa los servicios de SQL Server 2005 en los servidores SQL Server 2005. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Database - SQL Server 2008 Optional Services - {Severity3}**
  - Supervisa los servicios opcionales de SQL Server 2008 en los servidores SQL Server 2008. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Database - SQL Server 2008 Services - {Severity3}**
  - Supervisa los servicios de SQL Server 2008 en los servidores SQL Server 2008. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Correo Electrónico

- **Email - Blackberry Server Performance - {Severity2}**
  - Supervisa el rendimiento del servidor Blackberry en los servidores Blackberry. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Email - BlackBerry Server Services - {Severity3}**
  - Supervisa los servicios del servidor Blackberry en los servidores Blackberry. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange 2003 Services - {Severity3}**
  - Supervisa los servicios de Exchange 2003 en los servidores Exchange 2003. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange 2007 Services - {Severity3}**
  - Supervisa los servicios de Exchange 2007 en los servidores Exchange 2007. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange 2010 Edge Transport Queues - {Severity0}**

- Recolecta contadores de rendimiento de colas de Exchange 2010 Edge Transport en servidores Exchange 2010. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.

- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity2}**
  - Supervisa el rendimiento de colas en Exchange 2010 Edge Transport en los servidores Exchange 2010. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity3}**
  - Supervisa el rendimiento de colas en Exchange 2010 Edge Transport en los servidores Exchange 2010. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange 2010 Services - {Severity3}**
  - Supervisa los servicios de Exchange 2010 en las máquinas Exchange 2010. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange Client Active Logons - {Severity0}**
  - Recolecta contadores de rendimiento de inicios de sesión activos de clientes Exchange en los servidores Exchange. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Email - Exchange IMAP4 Service - {Severity3}**
  - Supervisa el servicio Exchange IMAP4 en los servidores Exchange. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange POP3 Service - {Severity3}**
  - Supervisa el servicio Exchange POP3 en los servidores Exchange. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange Server (Core) Performance - {Severity2}**
  - Supervisa el rendimiento de Exchange Server en los servidores Exchange. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Email - Exchange Server (Core) Services - {Severity3}**
  - Supervisa los servicios de Exchange Server (básico) en las máquinas con servidor Exchange (básico). Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - Exchange Server (Core) Store and Database - {Severity0}**
  - Recolecta contadores de rendimiento de almacenamiento y base de datos de Exchange Server en los servidores Exchange. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Email - SMTP Queue Performance - {Severity3}**
  - Supervisa el rendimiento de colas SMTP en los servidores SMTP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Email - SMTP Server Service - {Severity3}**
  - Supervisa el servicio de servidor SMTP en los servidores SMTP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Archivo/impresión

- **File / Print - DFS Service - {Severity3}**

- Supervisa el servicio DFS en las máquinas DFS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

- **File / Print - DFSR Service - {Severity3}**
  - Supervisa el servicio DFS en las máquinas DFSR. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **File / Print - NTFRS Service - {Severity3}**
  - Supervisa el servicio NTFRS en las máquinas NTFRS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **File / Print - Print Queue Job Errors Performance - {Severity1}**
  - Supervisa el rendimiento de errores en trabajos en colas de impresión en los servidores de archivos e impresión. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **File / Print - Spooler Service - {Severity3}**
  - Supervisa el servicio del administrador de trabajos en cola en los servidores de archivos e impresión. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Infraestructura de red

- **Network Infrastructure - Active Directory Domain Controller Services - {Severity3}**
  - Supervisa los servicios de controlador de dominio de Active Directory en los controladores de dominio de Active Directory. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Network Infrastructure - AD Domain Controller Performance - {Severity2}**
  - Supervisa el rendimiento del controlador de dominio de AD en los controladores de dominio de Active Directory. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Network Infrastructure - DHCP Server Performance - {Severity2}**
  - Supervisa el rendimiento del servidor DHCP en los servidores DHCP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Network Infrastructure - DHCP Server Service - {Severity3}**
  - Supervisa el servicio del servidor DHCP en los servidores DHCP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Network Infrastructure - DNS Server Performance - {Severity2}**
  - Supervisa el rendimiento del servidor DNS en los servidores DNS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Network Infrastructure - DNS Server Service - {Severity3}**
  - Supervisa el servicio del servidor DNS en los servidores DNS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Network Infrastructure - WINS Server Service - {Severity3}**
  - Supervisa el servicio del servidor WINS en los servidores WINS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Disk Space.Disk Space

- **Windows (Core) - Free Disk Space on Any Drive Below 1GB - {Severity2}**
  - Supervisa el espacio libre en disco en cualquier unidad por debajo de 1 GB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Windows (Core) - Free Disk Space on Any Drive Below 2GB - {Severity1}**
  - Supervisa el espacio libre en disco en cualquier unidad por debajo de 2 GB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Disk Space on Any Drive Below 750MB - {Severity3}**
  - Supervisa el espacio libre en disco en cualquier unidad por debajo de 750 MB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive C - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad C de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive C Below 1GB - {Severity2}**
  - Supervisa el espacio libre en disco en la unidad C por debajo de 1 GB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Windows (Core) - Free Disk Space on Drive C Below 750MB - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad C por debajo de 750 MB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive D - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad D de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive E - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad E de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive F - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad F de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Disk Space on Drive G - {Severity3}**
  - Supervisa el espacio libre en disco en la unidad G de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows (Core) - Free Space on C Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad C por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Space on C Drive Below 2GB - {Severity1}**
  - Supervisa el espacio libre en disco en la unidad C por debajo de 2 GB de las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).

- **Windows (Core) - Free Space on D Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad D por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Space on E Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad E por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Space on F Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad F por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows (Core) - Free Space on G Drive Below 15 Percent - {Severity1}**
  - Supervisa el espacio libre en la unidad G por debajo del 15 % en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).

Windows (principal)

- **Windows (Core) - All Automatic Services - {Severity0}**
  - Recolecta el estado del servicio de todos los servicios automáticos en las máquinas Windows. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Windows (Core) - CPU and Memory - {Severity0}**
  - Recolecta contadores de rendimiento de CPU y memoria en las máquinas Windows. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Windows (Core) - Machine Health - {Severity0}**
  - Recolecta contadores de rendimiento del estado de la máquina en las máquinas Windows. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Windows (Core) - Processor and Memory Performance - {Severity2}**
  - Supervisa el rendimiento del procesador y la memoria en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Windows (Core) - TCPv4 Connections Performance - {Severity2}**
  - Supervisa el rendimiento de las conexiones TCPv4 en las máquinas Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).

Servidores Windows

- **Windows Server (Core) - Cluster Services - {Severity3}**
  - Supervisa los servicios de clúster en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows Server (Core) - Disk Time and Queue Length Performance - {Severity2}**
  - Supervisa el rendimiento del tiempo de disco y la longitud de la cola en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).
- **Windows Server (Core) - Drive C Performance - {Severity1}**
  - Supervisa el rendimiento de la unidad C en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).

- **Windows Server (Core) - General System Performance - {Severity1}**
  - Supervisa el rendimiento general del sistema en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows Server (Core) - Server Reboots - {Severity1}**
  - Supervisa los reinicios del servidor en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows Server (Core) - Standard Services - {Severity3}**
  - Supervisa los servicios estándar en los servidores Windows. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows Server 2003 - Standard Services - {Severity3}**
  - Supervisa los servicios estándar en las máquinas con Windows Server 2003. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows Server 2008 - Standard Services - {Severity3}**
  - Supervisa los servicios estándar en las máquinas con Windows Server 2008. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Windows Server 2012 - Standard Services - {Severity3}**
  - Descripción: Supervisa los servicios estándar en las máquinas con Windows Server 2012. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Estaciones de trabajo Windows

- **Windows 7 - Standard Services - {Severity1}**
  - Supervisa los servicios estándar en las máquinas con Windows 7. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows 8 - Standard Services - {Severity1}**
  - Supervisa los servicios estándar en las máquinas con Windows 8. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows Vista - Standard Services - {Severity1}**
  - Supervisa los servicios estándar en las máquinas con Windows Vista. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).
- **Windows XP - Standard Services - {Severity1}**
  - Supervisa los servicios estándar en las máquinas con Windows XP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 1 (Severity1).

Acceso remoto

- **Remote Access - Citrix Licensing Service - {Severity3}**
  - Supervisa el servicio de licencia de Citrix en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Citrix Licensing WMI Service - {Severity3}**

  - Supervisa el servicio de licencia de Citrix WMI en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Citrix MetaFrame Services - {Severity3}**
  - Supervisa los servicios Citrix MetaFrame en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Citrix Server Services - {Severity3}**
  - Supervisa los servicios de los servidores Citrix en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Citrix Virtual Memory Optimization Service - {Severity3}**
  - Supervisa el servicio de optimización de memoria virtual Citrix en los servidores Citrix. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Terminal Server Services - {Severity3}**
  - Supervisa los servicios de los servidores Terminal Server en los servidores Terminal Server. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Remote Access - Terminal Server Session Performance - {Severity2}**
  - Supervisa el rendimiento de sesión de los servidores Terminal Server en los servidores Terminal Server. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 2 (Severity2).

Seguridad y antivirus

- **AV - AVG Tech AVG Services - {Severity3}**
  - Supervisa los servicios de AVG Technologies en las máquinas con protección AVG Technologies. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - McAfee Enterprise Services - {Severity3}**
  - Supervisa los servicios de McAfee Enterprise en las máquinas con protección McAfee Enterprise. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Microsoft SE-FEP Services {Severity3}**
  - Supervisa los servicios SE-FEP de Microsoft en equipos Microsoft SE-FEP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3)
- **AV - Sophos Antivirus Services - {Severity3}**
  - Supervisa los servicios de Sophos Antivirus en las máquinas con protección Sophos. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Symantec Antivirus Services - {Severity3}**
  - Supervisa los servicios de Symantec Antivirus en las máquinas con protección Symantec. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Symantec Endpoint Protection Services - {Severity3}**
  - Supervisa los servicios de Symantec Endpoint Protection en las máquinas con protección Symantec Endpoint Protection. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **AV - Trend Micro Client Server Security Services - {Severity3}**

- Supervisa los servicios Trend Micro Client/Server Security en las máquinas con protección Trend Micro Client/Server Security. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

- **AV - Trend Micro OfficeScan Services - {Severity3}**
  - Supervisa los servicios Trend Micro OfficeScan en las máquinas con protección Trend Micro OfficeScan. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Sistemas web

- **Web Systems - FTP Server Service - {Severity3}**
  - Supervisa el servicio del servidor FTP en los servidores FTP. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Web Systems - IIS Performance - {Severity3}**
  - Supervisa el rendimiento de IIS en los servidores IIS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Web Systems - IIS Server - {Severity0}**
  - Recolecta contadores de rendimiento del servidor IIS en los servidores IIS. Sólo se usa con la finalidad de mostrar los registros de monitor y elaborar informes.
- **Web Systems - IIS Server Services - {Severity3}**
  - Supervisa los servicios del servidor IIS en los servidores IIS. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).
- **Web Systems - SharePoint Server Services - {Severity3}**
  - Supervisa los servicios del servidor SharePoint en los servidores SharePoint. Se usa con la finalidad de mostrar los registros de monitor, elaborar informes y alertar. Las alarmas se consideran de gravedad 3 (Severity3).

Conjuntos de Eventos

Seguridad y antivirus

- **zz[SYS] AV - McAfee Anti-Virus (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de antivirus McAfee en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] AV - Microsoft SE-FEP (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de Microsoft Security Essentials y Forefront Endpoint Protection en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] AV - Microsoft SE-FEP (I) - SYS - {Severity0}**
  - Supervisa eventos específicos de información de Microsoft Security Essentials y Forefront Endpoint Protection en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] AV - Misc AntiVirus (EW) - APP-SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de antivirus diversos en los registros de eventos de la aplicación y del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] AV - Misc AntiVirus (I) - APP-SYS - {Severity1}**

- Supervisa eventos específicos de información de antivirus diversos en los registros de eventos de la aplicación y del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de antivirus Symantec y Norton en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de antivirus Symantec y Norton en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de antivirus Symantec y Norton en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] AV - Symantec/Norton AntiVirus (I) - APP - {Severity0}**
  - Supervisa eventos específicos de información de antivirus Symantec y Norton en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.

Respaldo

- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de Backup Exec en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de Backup Exec en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de Backup Exec en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Backup - Backup Exec (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de Backup Exec en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Backup - Backup Exec (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de Backup Exec en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Backup - Backup Exec Job Failure/Cancellation (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores por cancelaciones o errores de trabajo de Backup Exec en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Backup - Backup Exec Job Success (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de trabajos realizados correctamente de Backup Exec en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Backup - BrightStor ARCserve (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de BrightStor ARCserve en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Backup - BrightStor ARCServe (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de BrightStor ARCserve en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Backup - Microsoft Windows Backup (E) - APP - {Severity2}**

- Supervisa eventos específicos de errores de Microsoft Windows Backup en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).

- **zz[SYS] Backup - Misc Backup (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores de copia de seguridad diversos en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Backup - Misc Backup (I) - APP - {Severity0}**
  - Supervisa eventos específicos de información de copia de seguridad diversos en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Backup - Misc Backup (W) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias de copia de seguridad diversas en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).

Base de datos

- **zz[SYS] Database - SQL Server (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de las características ACID de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de las características ACID de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de las características ACID de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - ACID (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de las características ACID de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de las copias de seguridad de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de las copias de seguridad de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - Backup (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de las copias de seguridad de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de los recursos de base de datos de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de los recursos de base de datos de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de los recursos de base de datos de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - DB Resources (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de los recursos de base de datos de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del MSDTC de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del MSDTC de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del MSDTC de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - MSDTC (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos del MSDTC de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de red de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de red de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de consultas de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de consultas de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de las replicaciones de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de las replicaciones de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de las replicaciones de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server - Replication (EWISFCV) - APP - {Severity0}**

- Supervisa eventos específicos de las replicaciones de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.

- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de elaboración de informes de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de elaboración de informes de SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server - Reporting (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de elaboración de informes de SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de varias instancias del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de varias instancias del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de varias instancias del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de varias instancias del Agente SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de instancia única del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de instancia única del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de instancia única del Agente SQL Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Database - SQL Server Agent - Single Instance (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de instancia única del Agente SQL Server en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Database - SQL Server Cluster (I) - SYS - {Severity2}**
  - Supervisa eventos específicos de información de clúster de SQL Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Database - SQL/Service Control Manager (EW) - SYS - {Severity3}**

- Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de SQL Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).

Correo Electrónico

- **zz[SYS] Email - Blackberry Server (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Blackberry Server Events (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de eventos del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Blackberry Server Events (W) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias de eventos del servidor Blackberry en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2000 and 2003 (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores de Exchange 2000 y 2003 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2000 y 2003 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2000 y 2003 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2000 and 2003 and 2007 (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2000, 2003 y 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de Exchange 2007 en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de acceso de clientes de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de acceso de clientes de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de acceso de clientes de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Edge Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Edge Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Edge Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Hub Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Hub Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Exchange 2007 con el rol Hub Transport en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de buzón de correo de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de buzón de correo de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de buzón de correo de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Mailbox (EWISFCV) - APP - {Severity0}**
  - Supervisa eventos específicos de buzón de correo de Exchange 2007 en el registro de eventos de la aplicación. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity1}**

- Supervisa eventos específicos de errores y advertencias de los servicios Transport de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de los servicios Transport de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de los servicios Transport de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias del servicio de mensajería unificada de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias del servicio de mensajería unificada de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias del servicio de mensajería unificada de Exchange 2007 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange 2010 Server (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores del servidor Exchange 2010 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias del servidor Exchange 2010 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias del servidor Exchange 2010 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity3}**
  - Supervisa eventos específicos de advertencias del servidor Exchange 2010 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de Exchange Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de Exchange Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange Server (I) - SYS - {Severity3}**
  - Supervisa eventos específicos de información de Exchange Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange Server 5.5 (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de Exchange Server 5.5 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Email - Exchange/Service Control Manager (EW) - SYS - {Severity3}**

- Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de Exchange en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).

- **zz[SYS] Email - SMTP/Service Control Manager (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de SMTP en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).

Hardware

- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de las baterías Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de las baterías Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de las baterías Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Battery (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de las baterías Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del controlador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del controlador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del controlador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Controller (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos del controlador de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores eléctricos de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores eléctricos de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores eléctricos de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Electrical (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos eléctricos específicos de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de gabinetes Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity2}**

- Supervisa eventos específicos de advertencias y errores de gabinetes Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).

- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de gabinetes Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Enclosure (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de gabinetes Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de entorno de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de entorno de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de entorno de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Environmental (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de entorno de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del ventilador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del ventilador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del ventilador de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Fan (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos del ventilador de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con cambios en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con cambios en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores relacionados con cambios en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Hardware Changes (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos relacionados con cambios en el hardware de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity1}**

  - Supervisa eventos específicos de advertencias y errores relacionados con registros en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con registros en el hardware de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Hardware Log (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos relacionados con registros en el hardware de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de medios de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de medios de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de medios de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Media (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de medios de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con fallas previas en memorias de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con fallas previas en memorias de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSA en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSA en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSA en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell OMSA System (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos del sistema Dell OMSA en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSM en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del sistema Dell OMSM en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity1}**

- Supervisa eventos específicos de advertencias y errores relacionados con discos físicos Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos físicos Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos físicos Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Physical Disk (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos relacionados con discos físicos Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con la administración de energía de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores relacionados con la administración de energía de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores relacionados con la administración de energía de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Power Management (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de administración de energía de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 0 (Severity0).
- **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores del procesador Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del procesador Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Processor (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos del procesador Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de máquinas espejo para redundancia de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de máquinas espejo para redundancia de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Redundancy Mirror (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de máquinas espejo para redundancia de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.

- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores de temperatura de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores de temperatura de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de temperatura de Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Temperature (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de temperatura de Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos virtuales Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores relacionados con discos virtuales Dell en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - Dell Virtual Disk (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos relacionados con discos virtuales Dell en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Hardware - HP Top Tools (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de HP Top Tools en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - HP/Compaq Insight Manager (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de HP/Compaq Insight Manager en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - HP/Compaq StorageWorks (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores de HP/Compaq StorageWorks en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Hardware - IBM SeriesX Events (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de eventos de IBM SeriesX en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de hardware diversos en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Hardware - Misc HW (E) - SYS - {Severity2}**
  - Supervisa eventos específicos de errores de hardware diversos en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Hardware - Misc HW (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias de hardware diversas en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

Infraestructura de red

- **zz[SYS] Network Infrastructure - Active Directory (E) - SYS - {Severity1}**

- Supervisa eventos específicos de errores de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Network Infrastructure - Active Directory Events (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de eventos de Active Directory en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Network Infrastructure - Active Directory Events (W) - APP - {Severity2}**
  - Supervisa eventos específicos de advertencias de eventos de Active Directory en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Network Infrastructure - Active Directory Logon/Logoff/Lockout Activity (F) - SEC - {Severity3}**
  - Supervisa eventos específicos de auditoría de errores en la actividad de inicio de sesión, cierre de sesión y bloqueo de Active Directory en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores NTDS de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores NTDS de Active Directory en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Network Infrastructure - Active Directory NTDS (I) - SYS - {Severity0}**
  - Supervisa eventos específicos de información de NTDS de Active Directory en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] Network Infrastructure - DHCP Server (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de servidores DHCP en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - DHCP Server (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias de servidores DHCP en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - DNS Server (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de servidores DNS en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - DNS Server (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias de servidores DNS en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Network Infrastructure - WINS Server (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores de servidores WINS en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

Acceso remoto

- **zz[SYS] Remote Access - Citrix MetaFrame (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Citrix MetaFrame en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Remote Access - Citrix Server Events (E) - APP - {Severity2}**

- Supervisa eventos específicos de errores de eventos del servidor Citrix en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).

- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de eventos del servidor Terminal Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de eventos del servidor Terminal Server en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).

Sistemas web

- **zz[SYS] Web Systems - IIS 6 Events (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de IIS 6 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity2}**
  - Supervisa eventos específicos de errores de eventos de IIS 7 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity3}**
  - Supervisa eventos específicos de errores de eventos de IIS 7 en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] Web Systems - IIS Server (E) - APP - {Severity1}**
  - Supervisa eventos específicos de errores del servidor IIS en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] Web Systems - IIS Server (W) - APP - {Severity1}**
  - Supervisa eventos específicos de advertencias del servidor IIS en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 1 (Severity1).

Plataformas de SO

- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity2}**
  - Supervisa eventos específicos de errores comunes de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores comunes de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server (Core) Events (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos comunes de Windows Server en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity1}**
  - Supervisa eventos específicos de auditoría de errores comunes de Windows Server en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity3}**
  - Supervisa eventos específicos de auditoría de errores comunes de Windows Server en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias comunes de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias comunes de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server (Core) Ignore Events - (EW) - APP-SYS - {Ignore}**

- Omite los ajustes de supervisión de eventos específicos de errores y advertencias comunes de Windows Server en los registros de eventos de la aplicación y del sistema.

- **zz[SYS] OS - Windows Server (Core) Printer Spooler (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del administrador de trabajos de impresión de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de advertencias y errores del administrador de control de servicios de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (I) - SYS - {Severity2}**
  - Supervisa eventos específicos de información del administrador de control de servicios de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server (Core) System Shutdown (W) - SYS - {Severity2}**
  - Supervisa eventos específicos de advertencias relacionadas con el apagado del sistema de Windows Server en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores comunes de Windows Server 2008 en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores comunes de Windows Server 2008 en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server 2008 (Core) Events (W) - SYS - {Severity1}**
  - Supervisa eventos específicos de advertencias comunes de Windows Server 2008 en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos de la aplicación. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity3}**

- Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (avanzado) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).

- **zz[SYS] OS - Windows Server 2008 Advanced (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de Windows Server 2008 (avanzado) en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (básico) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity2}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (básico) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity3}**
  - Supervisa eventos específicos de errores y advertencias de Windows Server 2008 (básico) en el registro de eventos del sistema. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Server 2008 Basic (EWISFCV) - SYS - {Severity0}**
  - Supervisa eventos específicos de Windows Server 2008 (básico) en el registro de eventos del sistema. Sólo se usa para elaborar registros e informes.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity1}**
  - Supervisa eventos específicos de auditoría de errores de Windows Server 2008 (básico) en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 1 (Severity1).
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity2}**
  - Supervisa eventos específicos de auditoría de errores de Windows Server 2008 (básico) en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 2 (Severity2).
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity3}**
  - Supervisa eventos específicos de auditoría de errores de Windows Server 2008 (básico) en el registro de eventos de seguridad. Las alarmas se consideran de gravedad 3 (Severity3).
- **zz[SYS] OS - Windows Workstation (Core) Events (E) - SYS - {Severity1}**
  - Supervisa eventos específicos de errores comunes de estaciones de trabajo Windows en el registro de eventos del sistema. Las alarmas se consideran de gravedad 1 (Severity1).

Índice