**Introducción**

Microsoft Azure proporciona una solución avanzada de supervisión y de alertas denominada Azure Monitor. Puede utilizarse Azure Monitor para configurar notificaciones y alertas para los sistemas y aplicaciones clave. Estas alertas garantizan que el equipo apropiado sepa cuándo surge un problema.

Trabaja para una gran empresa de transporte que ha implementado recientemente varias aplicaciones web en la plataforma de Azure. Debido a un error de configuración, el seguimiento de pedidos accesible para los clientes estaba sin conexión. El problema no se identificó hasta que los clientes no empezaron a quejarse de que no podían realizar un seguimiento de sus pedidos. Como consecuencia, la satisfacción de los clientes con su servicio descendió.

Como arquitecto de soluciones de Azure para su empresa, debe encontrar una solución que detecte problemas en sus entornos en tiempo real. El equipo correcto recibirá una notificación para que pueda resolver cualquier problema antes de que los clientes se den cuenta.

**Objetivos de aprendizaje**

En este módulo, aprenderá a:

* Explorar las alertas mediante Azure Monitor.
* Comprender cuándo se usan los eventos de métrica, de registro y de registro de actividad.
* Crear y usar registros, métricas y alertas de registro de actividad.
* Use grupos de acciones para determinar qué tipo de notificaciones se envían y a quién.
* Obtenga información sobre cómo usar reglas de procesamiento de alertas para invalidar el comportamiento normal de los grupos de acciones cuando sea necesario.

**Requisitos previos**

* Conocimientos de Azure Monitor

**Exploración de los distintos tipos de alerta que admite Azure Monitor**

Azure Monitor es una herramienta eficaz de análisis y creación de informes. Puede usarla para obtener información sobre el comportamiento y la ejecución de su entorno y sus aplicaciones. De este modo, podrá responder de forma proactiva a los errores del sistema.

Tras el tiempo de inactividad al que se enfrentaron los clientes, configuró la supervisión de los recursos clave en Azure. Con la supervisión configurada, quiere asegurarse de que las personas correctas reciban alertas en el nivel adecuado.

En esta unidad, aprenderá cómo Azure Monitor recibe datos de recursos, cuáles son los componentes de una alerta y cómo y cuándo usar una. Por último, aprenderá a crear y administrar sus propias alertas.

**Tipos de datos en Azure Monitor**

Azure Monitor recibe datos de recursos de destino, como aplicaciones, sistemas operativos, recursos de Azure, suscripciones a Azure e inquilinos de Azure. La naturaleza del recurso define los tipos de datos que están disponibles. Un tipo de datos será una *métrica*, un *registro*, o bien una métrica y un registro:

* Los tipos de datos basados en *métricas* se centran en los valores numéricos que dependen del tiempo y que representan algún aspecto del recurso de destino.
* Los tipos de datos basados en *registros* se centran en la consulta de los datos de contenido en archivos de registro estructurados y basados en registros que son pertinentes para el recurso de destino.

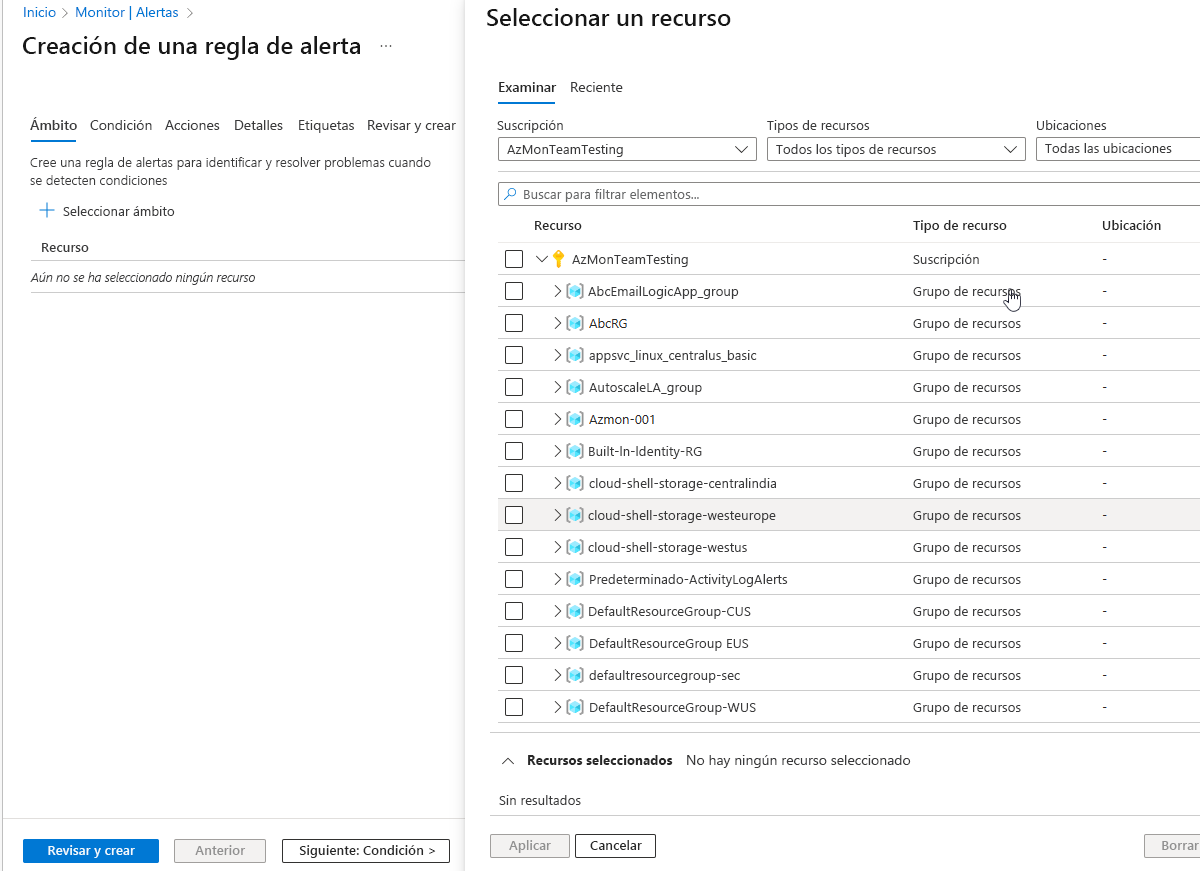
Aprenderá sobre los tres tipos de señal que puede usar para supervisar su entorno:

* Las alertas de **métricas** proporcionan un desencadenador de alertas para cuando se supera un umbral especificado. Por ejemplo, una alerta de métrica puede notificarle cuando el uso de CPU sea superior al 95 %.
* Las alertas de **registro de actividad** le notifican cuando los recursos de Azure cambian de estado. Por ejemplo, una alerta del registro de actividad puede recibir una notificación cuando se elimina un recurso.
* Las alertas de **registro** se basan en las cosas escritas en los archivos de registro. Por ejemplo, una alerta de registro puede notificarle cuando un servidor web haya devuelto varias respuestas 404 o 500.

**Composición de una regla de alertas**

Cada alerta o notificación disponible en Azure Monitor es producto de una regla. Algunas de estas reglas están integradas en la plataforma de Azure. Puede usar las reglas de alertas para crear alertas y notificaciones personalizadas. Independientemente del recurso de destino o del origen de datos que use, la composición de una regla de alertas sigue siendo la misma.

* **RECURSO**
  + El *recurso de destino* para la regla de alertas. Puede asignar varios recursos de destino a una única regla de alertas. El tipo de recurso define los tipos de señales disponibles.
* **CONDICIÓN**
  + El *tipo de señal* que se va a usar para evaluar la regla. El tipo de señal puede ser una métrica, un registro de actividad o de registros. Hay otros, pero no se tratan en este módulo.
  + La *lógica de alerta* aplicada a los datos proporcionados a través del tipo de señal. La estructura de la lógica de alerta cambia en función del tipo de señal.
* **ACCIONES**
  + La *acción*, como el envío de un correo electrónico, el envío de un mensaje SMS o el uso de un webhook.
  + Un *grupo de acciones*, que normalmente contiene un conjunto único de destinatarios para la acción.
* **DETALLES DE ALERTAS**
  + Un *nombre de alerta* y una *descripción de alerta* que especifican el propósito de la alerta.
  + La *gravedad* de la alerta si los criterios o la prueba de lógica tienen una evaluación true. Los cinco niveles de gravedad son:
    - **0**: Crítico
    - **1**: Error
    - **2**: Advertencia
    - **3**: Informativo
    - **4**: Detallado



**Ámbito de las reglas de alertas**

Puede obtener datos de supervisión a través de la mayoría de los servicios de Azure, y obtener informes sobre ellos mediante la canalización de Azure Monitor. En la canalización de Azure Monitor, puede crear reglas de alerta para los siguientes elementos, entre otros:

* Valores de métrica
* Consultas de búsqueda de registros
* Eventos del registro de actividad
* Estado de la plataforma Azure subyacente
* Pruebas de disponibilidad del sitio web

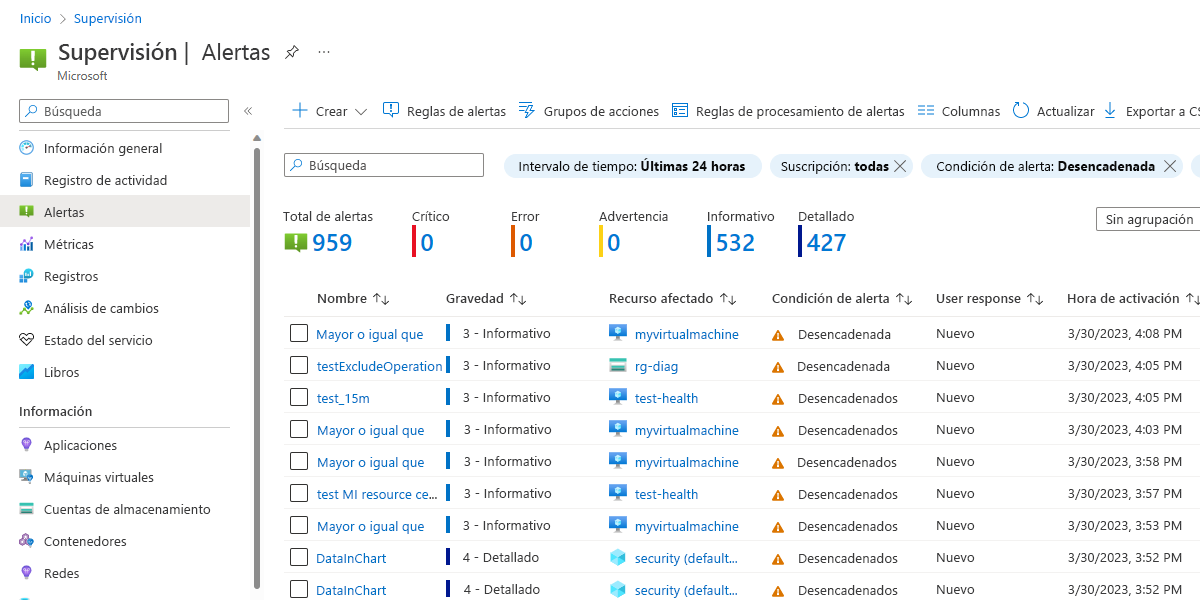
**Administración de reglas de alerta**

No todas las reglas de alertas que se crean deben ejecutarse indefinidamente. Con Azure Monitor, puede especificar una o varias reglas de alertas, y habilitarlas o deshabilitarlas, según sea necesario.

Como arquitecto de soluciones de Azure, puede usar Azure Monitor para habilitar alertas específicas y con un enfoque estricto antes de cualquier cambio en la aplicación. Después, las deshabilitaría tras una implementación correcta.

**Vista de resumen de las alertas**

La página de alerta muestra un resumen de todas las alertas. Puede aplicar filtros a la vista mediante el uso de una o varias de las categorías siguientes: suscripciones, condición de alerta, gravedad o intervalos de tiempo. En la vista solo se incluyen alertas que coinciden con estos criterios.



**Condición de alerta**

El sistema establece la condición de alerta.

* Cuando se desencadena una alerta, la condición de supervisión de la alerta se establece en **Desencadenada**.
* Después de que desaparece la condición subyacente que provocó que se activara la alerta, la condición de supervisión se establece en **Resuelta**.

Principio del formulario

**1. ¿De qué se compone una regla de alertas?**

1. Recurso, condición, registro y tipo de alerta.
2. Métricas, registros, aplicación y sistema operativo.
3. Recursos, condiciones, acciones y detalles de alertas.

**2. ¿Cuál de los siguientes constituye un ejemplo de un tipo de datos de registro?**

1. Porcentaje de CPU a lo largo del tiempo
2. Registros de respuesta HTTP
3. Tablas de la base de datos
4. Solicitudes de sitio web por hora
5. C
6. B

Final del formulario

**Uso de alertas de métricas sobre problemas de rendimiento en el entorno de Azure**

Azure Monitor puede usar umbrales para supervisar recursos específicos. En una organización, resulta mucho más útil recibir una notificación cuando el espacio libre en disco en un servidor es inferior al cinco por ciento a recibir una alerta cada vez que un archivo se guarde.

Como arquitecto de soluciones, quiere implementar la supervisión periódica de umbrales para una muchos de los recursos y las instancias de destino. La supervisión le ayudará a resolver posibles problemas antes de que afecten a sus clientes.

En esta unidad, investigará los distintos tipos de alertas de métricas que admite Azure Monitor.

**¿Cuándo se usan las alertas de métricas?**

En Azure Monitor, puede usar las alertas de métricas para realizar una supervisión periódica del umbral de los recursos de Azure. Azure Monitor ejecuta las condiciones del desencadenador de alertas de métricas a intervalos regulares. Cuando la evaluación es verdadera, Azure Monitor envía una notificación. Las alertas de métricas tienen estado y Azure Monitor solo enviará una notificación cuando se cumplan las condiciones de requisitos previos.

Las alertas de métricas pueden ser útiles si, por ejemplo, necesita saber cuándo el uso de la CPU del servidor alcanza un umbral crítico del 90 %. Puede que reciba una alerta cuando el espacio de almacenamiento de la base de datos sea demasiado reducido o cuando la latencia de red esté a punto de alcanzar niveles inaceptables.

**Composición de una alerta de métrica**

Como ha aprendido en la unidad anterior, todas las alertas se rigen por sus reglas. En el caso de las alertas de métricas, hay otro factor que se debe definir: el tipo de condición. que puede ser estático o dinámico.

Debe definir el tipo de análisis estadístico que se va a usar con las alertas de métricas estáticas o dinámicas. Los tipos de ejemplo son mínimo, máximo, promedio y total. En este ejemplo, define el período de datos que se va a evaluar: los últimos 10 minutos. Por último, establezca la frecuencia con la que se comprobarán las condiciones de la alerta: cada 2 minutos.

**Uso de alertas de métricas de umbral estático**

Las alertas de métricas estáticas se basan en las condiciones y los umbrales estáticos simples que define. Con las métricas estáticas, especifique el umbral que se usa para desencadenar la alerta o la notificación.

En el escenario definido previamente, una alerta estática con un umbral de uso de la CPU del 85 % comprueba la regla cada dos minutos. Analiza los últimos 10 minutos de datos de uso de la CPU para evaluar si este supera el umbral. Si la evaluación es verdadera, la alerta desencadena las acciones asociadas con el grupo de acciones.

**Uso de alertas de métricas de umbral dinámico**

Las alertas de métricas dinámicas usan herramientas de aprendizaje automático que proporciona Azure para mejorar automáticamente la precisión de los umbrales definidos por la regla inicial.

No hay ningún umbral estricto en las métricas dinámicas. Sin embargo, deberá definir dos parámetros más:

* El *período de retroceso* define el número de períodos anteriores que deben evaluarse. Por ejemplo, si establece el período de retroceso en 3, en el ejemplo que se usa aquí, el intervalo de datos evaluado sería de 30 minutos (tres conjuntos de 10 minutos).
* El *número de infracciones* expresa cuántas veces tiene que desviarse la condición lógica del comportamiento esperado antes de que la regla de alertas desencadene una notificación. En este ejemplo, si se establece el número de infracciones en 2, la alerta se desencadenaría después de dos desviaciones del umbral calculado.

**Descripción de las dimensiones**

Hasta ahora, las alertas de métricas evaluadas se han centrado en una única instancia de destino. Azure Monitor admite dimensiones, las cuales permiten proporcionar datos de supervisión de varias instancias de destino.

Las dimensiones se usan para definir una regla de alerta métrica y para aplicarla a varias instancias relacionadas. Por ejemplo, puede supervisar el uso de la CPU en todos los servidores que ejecutan la aplicación. Después, puede recibir una notificación individual para cada instancia del servidor cuando se desencadenen las condiciones de la regla.

Para definir las dimensiones, puede asignar un nombre a cada instancia de destino específicamente o emplear el carácter comodín asterisco (\*), que usa todas las instancias disponibles.

**Escala de alertas de métricas**

Igual que en el caso de las dimensiones, Azure Monitor admite la creación de alertas de métricas que supervisan varios recursos. El escalado está limitado actualmente a las máquinas virtuales de Azure. Sin embargo, una alerta de métrica individual puede supervisar los recursos de una sola región de Azure.

La creación de reglas de alertas de métricas de escalado para supervisar varios recursos no es diferente de la creación de cualquier otra regla de alertas de métricas; solo tiene que seleccionar todos los recursos que desea supervisar.

Igual que en el caso de las dimensiones, una alerta de métrica de escalado es individual para el recurso que la ha desencadenado.

**Uso de alertas de registro para alertar sobre eventos en la aplicación**

Puede usar Azure Monitor para capturar información importante de los archivos de registro. Estos archivos de registro pueden crearlos aplicaciones, sistemas operativos, otros tipos de hardware o servicios de Azure.

Como arquitecto de soluciones, quiere explorar las maneras en que la supervisión de los datos de registro puede a detectar problemas antes de que afecten a los clientes. Sabe que Azure Monitor admite el uso de datos de registro.

En esta unidad, comprenderá cómo el uso de los datos de registro puede mejorar la resistencia en el sistema.

**Cuándo se usan las alertas de registro**

Las alertas de registro usan los datos de registro para evaluar la lógica de la regla y, si es necesario, desencadenan una alerta. Estos datos pueden proceder de cualquier recurso de Azure, como registros de servidor, registros de servidor de aplicaciones o registros de aplicaciones.

Por su naturaleza, los datos de registro son históricos, de modo que el uso se centra en análisis y tendencias.

Puede usar estos tipos de registros para evaluar si alguno de los servidores ha superado su uso de CPU por un umbral determinado durante los últimos 30 minutos, o bien puede evaluar los códigos de respuesta emitidos en el servidor de aplicaciones web en la última hora.

**Funcionamiento de las alertas de registro**

Las alertas de registro se comportan de una manera ligeramente diferente a otros mecanismos de alerta. La primera parte de una alerta de registro define la regla de búsqueda de registros. Esta regla define la frecuencia con la que se debe ejecutar, el período de tiempo de evaluación y la consulta que se va a ejecutar.

Cuando una búsqueda de registro se evalúa como positiva, se crea un registro de alerta y se desencadenan las acciones asociadas.

**Composición de las reglas de búsqueda de registros**

Cada alerta de registro tiene una regla de búsqueda asociada. Estas reglas están compuestas por los siguientes elementos:

* **Consulta de registro**: consulta que se ejecuta cada vez que se activa la regla de alertas
* **Período de tiempo**: intervalo de tiempo para la consulta
* **Frecuencia**: frecuencia con la que se debe ejecutar la consulta
* **Umbral**: punto desencadenante para crear una alerta

Los resultados de la búsqueda de registros son de dos tipos: *número de registros* o *medición de métricas*.

**Número de registros**

Considere el uso del tipo número-de-registros como tipo de búsqueda de registros para trabajar con un evento o con datos basados en eventos. Algunos ejemplos son las respuestas de syslog y aplicaciones web.

Este tipo de búsqueda de registros devuelve una única alerta cuando el número de registros de un resultado de búsqueda alcanza o supera el valor del número de registros (umbral). Por ejemplo, si el umbral de la regla de búsqueda es mayor o igual que cinco, los resultados de la consulta tienen que devolver cinco o más filas de datos para que se desencadene la alerta.

**Unidades métricas**

Los registros de medición de métricas ofrecen la misma funcionalidad básica que los registros de alertas de métricas.

A diferencia de los registros de búsqueda de número-de-registros, los registros de medición de métricas requieren que se establezcan criterios adicionales:

* **Función de agregado**: define el cálculo que se realizará con los datos del resultado. Un ejemplo es el recuento o promedio. El resultado de la función se denomina **AggregatedValue**.
* **Campo de grupo**: campo por el que se va a agrupar el resultado. Este criterio se utiliza con el valor agregado. Por ejemplo, podría especificar que quiere que el promedio se agrupe por equipo.
* **Intervalo**: intervalo de tiempo en el que se agregan los datos. Por ejemplo, si especifica 10 minutos, se creará un registro de alerta para cada bloque agregado de 10 minutos.
* **Umbral**: definido por un valor agregado y el número total de infracciones.

Considere el uso de este tipo de alerta cuando necesite agregar un nivel de tolerancia a los resultados encontrados. Uno de los usos de este tipo de alerta es responder si se encuentra una tendencia o un patrón determinados. Por ejemplo, si el número de infracciones es cinco y un servidor del grupo supera el 85 % de uso de CPU más de cinco veces en el período de tiempo especificado, se activa una alerta.

Como puede ver, las mediciones de métricas reducen en gran medida el volumen de alertas que se producen. Sin embargo, preste especial atención a la hora de establecer los parámetros de umbral para que no falten alertas críticas.

**Naturaleza sin estado de las alertas de registro**

Una de las consideraciones principales cuando evalúa el uso de alertas de registro es que no tienen estado (las alertas de registro con estado están [actualmente en versión preliminar](https://learn.microsoft.com/es-es/azure/azure-monitor/alerts/alerts-types#log-alerts)). Una alerta de registro sin estado generará nuevas alertas cada vez que se activen los criterios de la regla, independientemente de si la alerta se ha registrado previamente.

**Uso de alertas de registro de actividad para alertar sobre eventos dentro de la infraestructura de Azure**

Las alertas de registro de actividad le permiten recibir notificaciones cuando se produce un evento específico en algún recurso de Azure. Por ejemplo, puede recibir una notificación cuando alguien cree una máquina virtual nueva en una suscripción.

Un registro de actividad también puede incluir alertas para el estado del servicio de Azure. Una empresa puede recibir notificaciones cuando se produzcan problemas en el servicio o se realice un mantenimiento planeado en la plataforma de Azure.

Como arquitecto de soluciones de Azure, quiere explorar la capacidad de supervisar recursos de Azure seleccionados en su suscripción. Aprenderá cómo puede usar los recursos para mejorar la capacidad de respuesta del equipo y la estabilidad de los sistemas.

En esta unidad explorará los dos tipos diferentes de alertas del registro de actividad. Ahora que ha visto los distintos tipos de alertas que puede usar en Azure Monitor, verá cómo puede desencadenar acciones para las alertas. Estas acciones pueden incluir el envío de un correo electrónico o la creación de una incidencia de IT Service Management (ITSM).

**Cuándo se usan las alertas de registro de actividad**

Hasta ahora, ha visto dos tipos diferentes de alertas que se admiten en Azure Monitor. Las *alertas de métricas* son ideales para supervisar las infracciones de umbral o detectar tendencias; las *alertas de registro*permiten una mayor supervisión analítica de los datos históricos.

Las alertas de registro de actividad están diseñadas para funcionar con recursos de Azure. Normalmente, es necesario crear este tipo de registro para recibir notificaciones si se producen cambios específicos en un recurso de la suscripción a Azure.

Hay dos tipos de alertas de registro de actividad:

* **Operaciones específicas**: se aplica a los recursos de la suscripción a Azure y, a menudo, tiene un ámbito con recursos específicos o un grupo de recursos. Utilizará este tipo cuando necesite recibir una alerta que informe de un cambio en un aspecto de su suscripción. Por ejemplo, puede recibir una alerta si se elimina una máquina virtual o se asignan nuevos roles a un usuario.
* **Eventos de estado del servicio**: incluyen la notificación de incidentes y el mantenimiento de los recursos de destino.

**Composición de una alerta de registro de actividad**

Es importante tener en cuenta que las alertas de registro de actividad solo supervisarán los eventos de la suscripción en la que se creó la alerta de registro.

Las alertas de registro de actividad se basan en eventos. El mejor método para definirlas es usar Azure Monitor para filtrar todos los eventos de la suscripción hasta que encuentre el que quiere. Para comenzar el proceso de creación, seleccione **Agregar alerta de registro de actividad**.

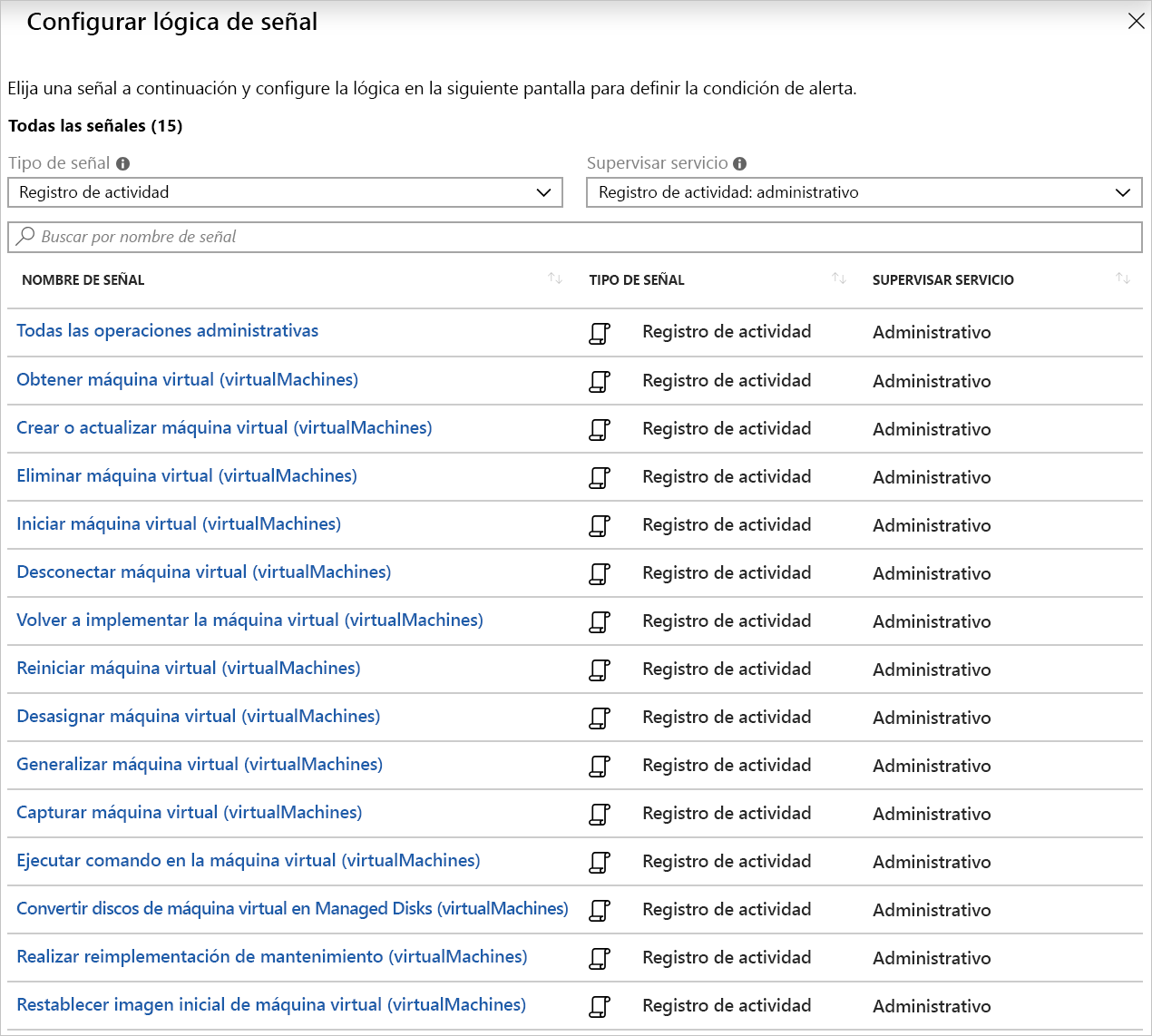
Igual que las alertas anteriores, las alertas de registro de actividad tienen sus propios atributos:

* **Categoría**: administración, mantenimiento del servicio, escalado automático o recomendación
* **Ámbito**: nivel de recursos, nivel de grupo de recursos o nivel de suscripción
* **Grupo de recursos**: donde se guarda la regla de alerta
* **Tipo de recurso**: espacio de nombres para el destino de la alerta
* **Nombre de la operación**: nombre de la operación
* **Nivel**: detallado, informativo, advertencia, error o crítico
* **Estado**: iniciado, erróneo o correcto
* **Evento iniciado por**: Dirección de correo electrónico o identificador de Microsoft Entra (conocido como "autor de llamada") para el usuario

**Creación de una alerta de registro específica del recurso**

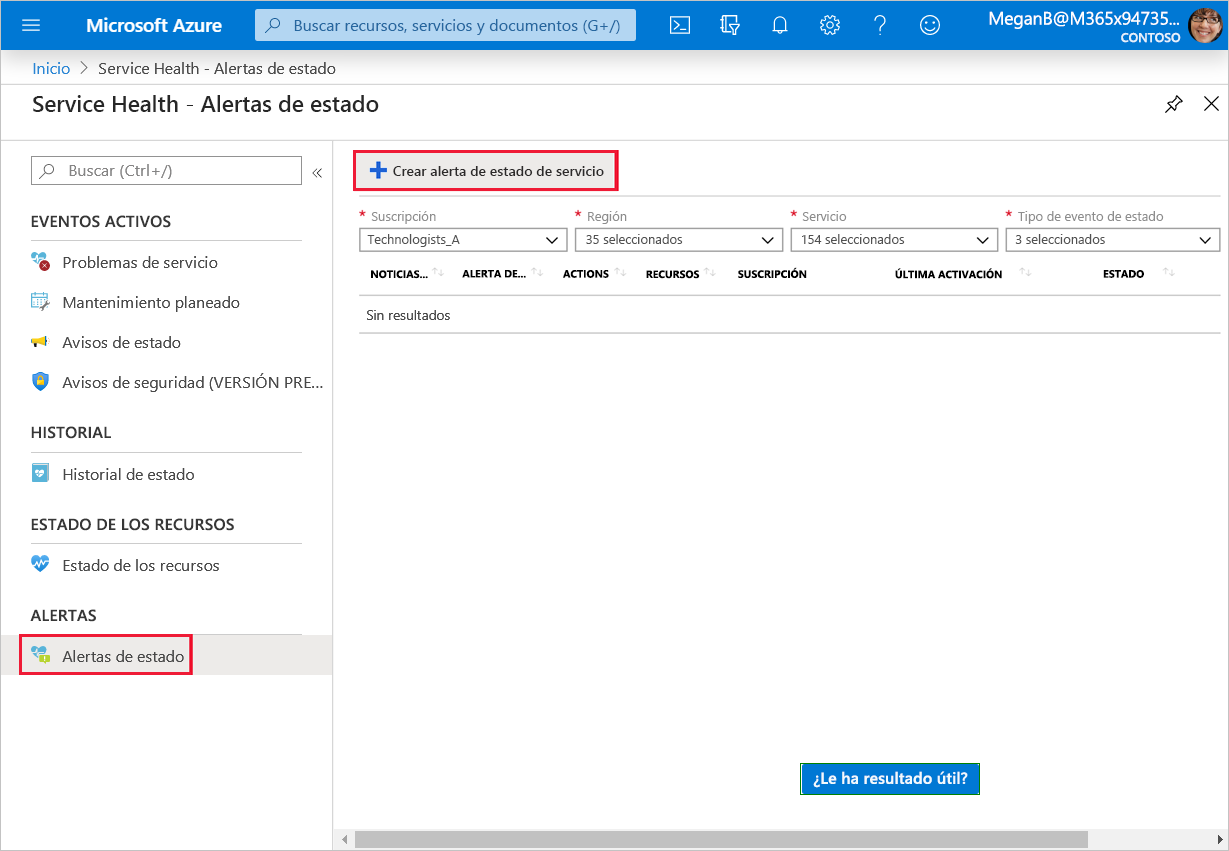
Cuando cree una alerta de registro de actividad, seleccione **Registro de actividad** para el tipo de señal. A continuación, verá todas las alertas disponibles para el recurso que seleccione. En la imagen siguiente se muestran todas las alertas administrativas de las máquinas virtuales de Azure. En este ejemplo, se desencadena una alerta al apagar una máquina virtual.

Si cambia el servicio de supervisión podrá reducir la lista de opciones. Si selecciona **Administración**, se filtran todas las señales para mostrar solo las relacionadas con el administrador.



**Creación de una alerta de Service Health**

Las alertas de estado del servicio no son como el resto de tipos de alerta que ha visto hasta ahora en este módulo. Para crear una nueva alerta busque y seleccione **Estado del servicio** en Azure Portal. A continuación, seleccione **Alertas de estado**. Después de seleccionar **Crear alerta de estado de servicio**, los pasos para crear la alerta son similares a los que ha visto para crear otras alertas.



La única diferencia es que ya no es necesario seleccionar un recurso, ya que la alerta es para toda una región de Azure. Lo que puede seleccionar es el tipo de evento de estado sobre el que quiere recibir alertas. Puede seleccionar incidencias de servicio, mantenimiento planeado o avisos de estado, o elegir todos los eventos. Los pasos restantes para realizar acciones y asignar nombres a las alertas son los mismos.

**Uso de grupos de acciones y reglas de procesamiento de alertas para enviar notificaciones cuando se desencadena una alerta**

Cuando se desencadena una alerta, Azure Monitor, Azure Service Health y Azure Advisor usan grupos de acciones para notificar a los usuarios estas alertas y llevar a cabo una acción. Un grupo de acciones es una colección de preferencias y acciones de notificación que se ejecutan cuando se desencadena la alerta. Puede ejecutar una o varias acciones para cada alerta desencadenada.

Azure Monitor puede realizar cualquiera de las siguientes acciones:

* Enviar un correo electrónico
* Enviar un mensaje SMS
* Crear una notificación de inserción para una aplicación de Azure
* Hacer una llamada de voz a un número
* Llamar a una función de Azure
* Desencadenar una aplicación lógica
* Enviar una notificación a un webhook
* Crear un vale de ITSM
* Usar un runbook (para reiniciar, o para escalar o reducir verticalmente una máquina virtual)

Una vez que haya creado un grupo de acciones, puede volver a usar ese grupo de acciones con la frecuencia que desee. Por ejemplo, después de crear una acción para enviar un correo electrónico al equipo de operaciones de su empresa, puede agregar ese grupo de acciones a todos los eventos de estado del servicio.

Mientras crea la regla de alertas, puede crear un nuevo grupo de acciones o agregar un grupo de acciones existente a la regla de alertas. También puede editar una alerta existente para agregar un grupo de acciones.

**Reglas de procesamiento de alertas**

Use reglas de procesamiento de alertas para invalidar el comportamiento normal de una alerta desencadenada agregando o suprimiendo un grupo de acciones. Puede usar reglas de procesamiento de alertas para agregar grupos de acciones o quitar (suprimir) grupos de acciones de las alertas desencadenadas. Las reglas de procesamiento de alertas son diferentes de las reglas de alerta. Las reglas de alertas desencadenan alertas cuando se cumple una condición en los recursos supervisados. Las reglas de procesamiento de alertas modifican las alertas a medida que se desencadenan.

Puede usar reglas de procesamiento de alertas para:

* Suprimir notificaciones durante las ventanas de mantenimiento planeado.
* Implemente la administración a escala especificando la lógica que se usa habitualmente en una sola regla, en lugar de tener que establecerla de forma coherente en todas las reglas de alerta.
* Agregar grupos de acciones a todos los tipos de alerta.

Las reglas de procesamiento de alertas se pueden aplicar a diferentes ámbitos de recursos, desde un único recurso a una suscripción completa. También permiten aplicar varios filtros o hacer que la regla funcione según una programación predefinida.

Puede controlar cuándo se aplica la regla de procesamiento de alertas. De forma predeterminada, la regla siempre está activa, pero puede seleccionar una ventana única para que esta regla se aplique, o bien puede haber establecido una periodicidad, como una periodicidad semanal.

**Resumen**

En este módulo, ha aprendido cómo le ayudan las alertas y notificaciones de Azure Monitor a administrar sus sistemas y entornos. Ha explorado tres tipos diferentes de alertas: de métricas, de registro y de registro de actividad.

Ha aprendido cómo las alertas de métricas habilitan las evaluaciones de series temporales que desencadenan un grupo de acciones cuando se activa la alerta.

También ha aprendido cómo las reglas de alertas de registro especifican las consultas de registro que deben ejecutarse a intervalos de tiempo regulares. Las alertas desencadenan un grupo de acciones cuando se encuentra una coincidencia.

Ha aprendido cómo las alertas del registro de actividad habilitan las notificaciones en los casos en los que un recurso de Azure con nombre cumple las condiciones especificadas.

Por último, ha aprendido a aplicar un grupo de acciones a una alerta para enviar notificaciones cuando se desencadena una alerta y a usar reglas de procesamiento de alertas para invalidar el comportamiento de un grupo de acciones cuando sea necesario.

**Limpieza**

El espacio aislado limpia los recursos automáticamente cuando haya terminado con este módulo.

Al trabajar en una suscripción propia, se recomienda identificar al final de un proyecto si aún necesita los recursos creados. Los recursos que dejas en ejecución pueden costar dinero. Puede eliminar los recursos de forma individual o eliminar el grupo de recursos para eliminar todo el conjunto de recursos.