**Introducción**

Las alertas de Azure Monitor proporcionan una manera de capturar datos de telemetría y detectar posibles problemas de infraestructura o aplicaciones.

Imagine que es administrador de TI para una gran empresa de comercio electrónico. Durante un evento de venta importante, se da cuenta de que el rendimiento del sitio web se está degradando, provocando tiempos de carga de página lentos y clientes frustrados. Necesita una manera de identificar y solucionar estos problemas de forma proactiva antes de que afecten a los usuarios. Mediante la configuración de alertas, es posible supervisar el rendimiento de la infraestructura y recibir notificaciones cuando se cumplan determinadas condiciones. Esto significa que podría tomar decisiones con capacidad de respuesta y garantizar una mejor experiencia del usuario.

En este módulo, aprenderá a configurar diferentes alertas en Azure Monitor. Los temas incluyen cómo crear reglas de alertas y grupos de acciones.

El objetivo de este módulo es proporcionarle los conocimientos y aptitudes necesarios para usar de forma eficaz las alertas de Azure Monitor.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Configurar alertas de Azure Monitor.
* Crear reglas de alertas y grupos de acciones.
* Notificar y supervisar alertas.

**Aptitudes evaluadas**

El contenido del módulo le ayuda a prepararse para el [examen AZ-104: Administrador de Microsoft Azure](https://learn.microsoft.com/es-es/certifications/exams/az-104).

**Descripción de las alertas de Azure Monitor**

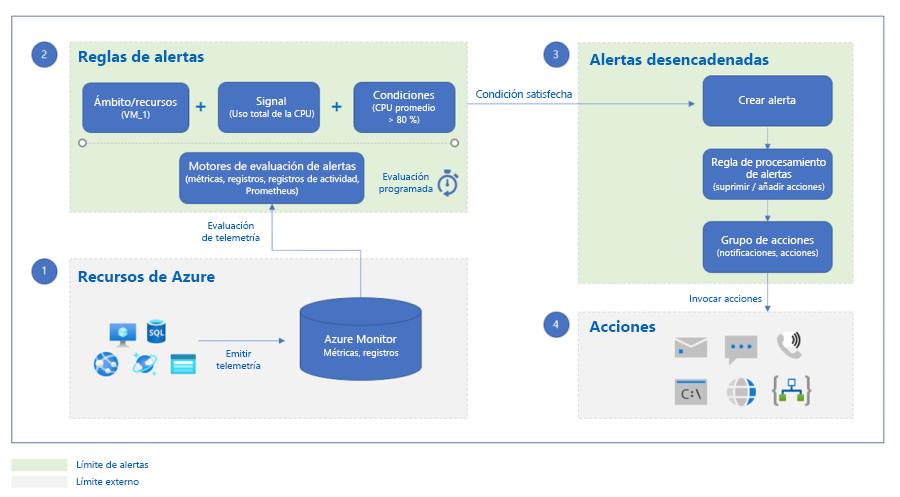
Azure Monitor captura los registros y los datos de telemetría de métricas de la infraestructura o las aplicaciones para poder analizar e identificar posibles problemas. Puede configurar alertas de Azure para iniciar una acción con capacidad de respuesta y enviar notificaciones basadas en los datos de telemetría. Las alertas de Azure le ayudan a detectar y solucionar problemas para mantener las aplicaciones en ejecución y evitar interrupciones del servicio para los usuarios.

**Aspectos que debe saber sobre las alertas de Azure**

Vamos a examinar cómo trabajar con alertas de Azure y Azure Monitor.

* En Azure Portal, configurará Azure Monitor para capturar los datos de telemetría de los servicios, recursos y aplicaciones de Azure.
* Cree alertas para que la configuración de Azure funcione con los datos de telemetría capturados.
* Una alerta consta de *reglas de alerta* que combinan la configuración y las condiciones que quiere supervisar, entre las que se incluyen:
  + Recursos para supervisar
  + Señales o telemetría para recopilar de los recursos
  + Condiciones que deben coincidir
* Una regla de alerta especifica *grupos de acciones* para cumplir los pasos con capacidad de respuesta cuando se desencadena una alerta, como enviar notificaciones.
* Cada alerta supervisa la telemetría y captura una señal sobre los cambios en el recurso especificado.
* La regla de alerta captura la señal y comprueba si la señal coincide con los criterios de condición.
* Cuando las condiciones de la regla coinciden con los datos de telemetría, una alerta se desencadena e invoca los grupos de acciones especificados.
* Si va a supervisar varios recursos, el sistema evalúa las condiciones por separado para cada recurso y las alertas se desencadenan para cada recurso por separado.

En el diagrama siguiente se muestra el proceso de alertas de Azure.

[](https://learn.microsoft.com/es-es/training/wwl-azure/configure-azure-alerts/media/how-azure-monitor-alerts-work-expanded.png#lightbox)

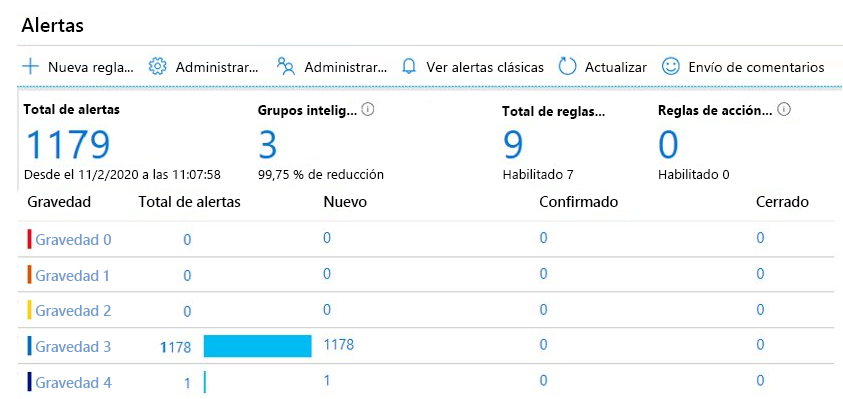
**Aspectos que se deben tener en cuenta al usar alertas de Azure**

La experiencia de alertas de Azure Monitor ofrece muchas ventajas. A medida que revise esta lista, tenga en cuenta cómo puede implementar alertas para mejorar la solución de supervisión y diagnóstico.

| **Prestación** | **Descripción** |
| --- | --- |
| **Sistema de notificaciones mejorado** | Implemente grupos de acciones para todas las alertas más recientes para acceder a las notificaciones. Defina notificaciones y otras acciones y reutilice esta configuración para varias alertas. |
| **Experiencia de creación unificada** | Cree fácilmente todas las alertas en un solo lugar. Siga el mismo proceso para configurar alertas de métricas, registros y registros de actividad en Azure Monitor, Log Analytics (en Azure Portal) y Azure Application Insights. |
| **Vista combinada para alertas de Log Analytics** | Supervise las alertas de Log Analytics para las suscripciones en Azure Portal, junto con los demás recursos y aplicaciones supervisados. Antes de la nueva experiencia de alertas de Azure, las alertas de Azure Monitor (Log Analytics) se mostraban en un portal independiente. |
| **Separación de las alertas activas y las reglas de alertas** | Diferencie entre las reglas de alerta con condiciones para desencadenar una alerta y la alerta activa (desencadenada). Separe las vistas operativas y de configuración de las alertas, las reglas de alertas y las acciones. |
| **Mejor flujo de trabajo** | Aproveche la nueva experiencia de creación de alertas de Azure que le guía por el proceso de configuración de reglas de alertas. Obtenga ayuda para detectar y definir la configuración y las condiciones para desencadenar las alertas. |

**Administración de las alertas de Azure Monitor**

Puede trabajar con alertas de Azure Monitor en Azure Portal. Hay opciones para crear y administrar las instancias de alerta, las reglas y condiciones de alerta y las acciones de respuesta de alertas.



Vamos a examinar algunos conceptos de alerta con más detalle.

**Aspectos que debe saber sobre los tipos de alerta**

Hay diferentes tipos de alertas para admitir diversos escenarios de configuración y supervisión, como métricas, registros y eventos. Las reglas de alerta se definen para los distintos tipos de telemetría recopilados de los orígenes de datos supervisados. Desencadene alertas según las condiciones de los datos de métricas y registros, o bien observando los eventos del registro de actividad. También puede implementar alertas para ayudar a mantener el estado de la plataforma Azure subyacente y probar la disponibilidad del sitio web.

Estos son algunos de los tipos de alerta más comunes:

* **Alertas de métricas**: evalúe los datos de métricas de los recursos a intervalos regulares. Recopile datos de métricas de la plataforma, los registros de Azure Monitor convertidos en métricas, Azure Application Insights y métricas personalizadas. Las alertas de métricas pueden aplicar varias condiciones y umbrales dinámicos.
* **Alertas de registro**: use consultas de Log Analytics en Azure Portal para evaluar los registros de recursos con una frecuencia predefinida.
* **Eventos del registro de actividad**: implemente alertas para desencadenarse cuando se produce un nuevo evento de registro de actividad que cumpla sus condiciones. Alertas de *Resource Health* y alertas de *Service Health* son dos tipos de alertas de registro de actividad.
* **Alertas de detección inteligente**: reciba advertencias automáticas sobre posibles problemas de rendimiento y anomalías de error en las aplicaciones web mediante la detección inteligente en los recursos de Application Insights. Migre la detección inteligente en los recursos de Application Insights para crear reglas de alerta para los distintos módulos de detección inteligente.

**Aspectos que debe saber sobre los estados de alerta**

En Azure Portal, cada alerta tiene un indicador de *estado* para identificar dónde se encuentran la alerta y el problema correspondiente en el proceso de supervisión.

* Hay tres estados de alerta:
  + **Nuevo**: el problema es nuevo (está abierto) y no está en revisión.
  + **Confirmado**: el problema está en revisión y el trabajo está en curso.
  + **Cerrado**: el problema se ha completado.
* Durante el proceso de supervisión de alertas, cuando las condiciones de una regla de alerta coinciden con los datos de telemetría del recurso especificado, se desencadena una alerta e invoca los grupos de acciones especificados. El sistema establece el estado de alerta en *Nuevo*.
* Una vez que el sistema establece un estado de alerta en *Nuevo*, puede cambiar el estado para especificar dónde se encuentra el problema relacionado en el proceso de resolución.

**Importante**

Solo el sistema establece el estado *Nuevo* inicial de una alerta. Todos los demás cambios de estado deben realizarse por usted como administrador.

* Cuando el problema de la alerta está en revisión, puede cambiar el estado de la alerta a *Confirmado*.
* Después de solucionar el problema de una alerta, puede cambiar el estado de la alerta a *Cerrado*.
* Si una alerta está en estado *Cerrado*, puede "volver a abrir" la alerta cambiando el estado de la alerta a *Nuevo* o *Confirmado*. |
* El historial de la alerta almacena todos los cambios de estado.

**Estado de alerta y condición de Azure Monitor**

El **estado de alerta** es diferente e independiente de la **condición** de Azure Monitor, como se muestra en Azure Portal.

* Tras el desencadenador inicial de una alerta, el sistema cambia el estado de la alerta a *Nuevo*. Un administrador local realiza todos los cambios adicionales en el estado de la alerta.
* Para todas las actualizaciones de la condición de Azure Monitor para la misma alerta, el sistema realiza todos los cambios.
* Cuando se desencadena una alerta, la condición de Azure Monitor para la alerta cambia a *activada*.
* Cuando se soluciona el problema de una alerta, la condición de Azure Monitor para la alerta cambia a *resuelta*.

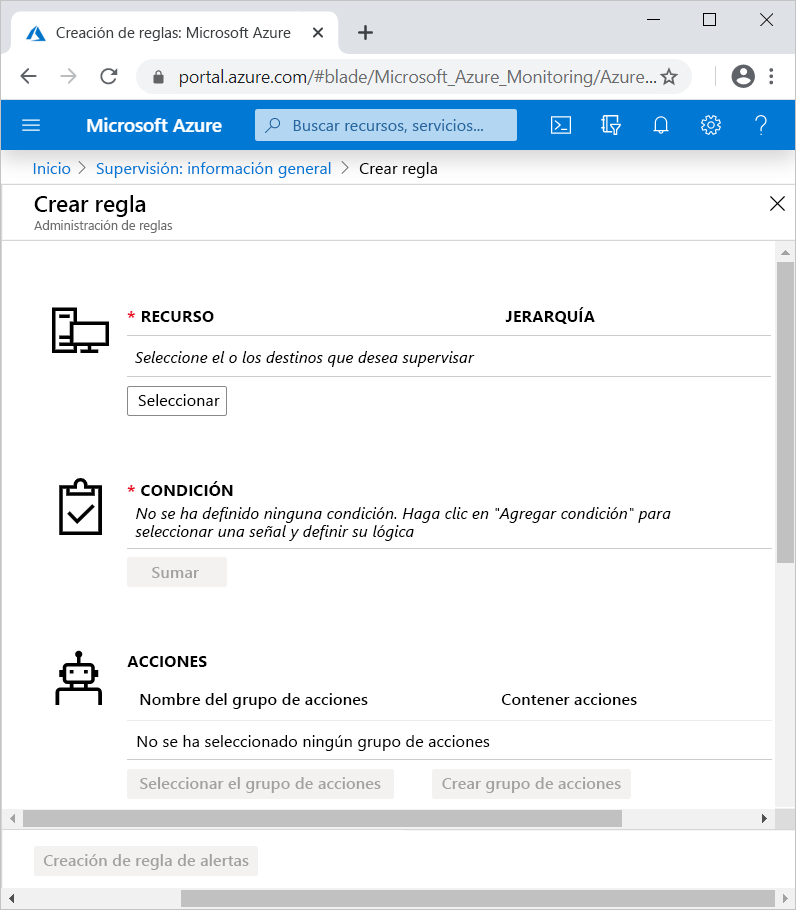
**Alertas con y sin estado**

Puede configurar la mayoría de los tipos de alertas como *con estado* o *sin estado*, que corresponde al número de instancias de la misma alerta que pueden estar activas al mismo tiempo.

* Las **alertas sin estado** se desencadenan cada vez que la condición de regla de alerta coincide con los datos, incluso si ya existe la misma alerta. Puede configurar alertas de registro y alertas de métricas como sin estado.
* Las **alertas con estado** se desencadenan cada vez que la condición de regla de alerta coincide con los datos y no existe la misma alerta. Una alerta con estado no desencadena más acciones hasta que se borren las condiciones de la regla de alerta actual. Puede configurar alertas de registro y alertas de métricas como con estado. Las alertas del registro de actividad nunca tienen estado.

**Creación de reglas de alerta**

Para crear una alerta en Azure Portal, debe definir una regla de alerta para la alerta. Las reglas de alertas constan de recursos, grupos de acciones y condiciones de supervisión que representan el destino y los criterios de la operación de alerta.



**Aspectos que debe saber sobre las reglas de alertas**

Echemos un vistazo más cercano a cómo crear y trabajar con reglas de alertas.

* Una regla de alerta consta de varios atributos clave: el recurso de destino, una señal de alerta, los criterios de regla, la gravedad del problema y un nombre y una descripción.
* El **recurso de destino** define el ámbito y las señales que están disponibles para la operación de alerta. Un destino puede ser cualquier recurso de Azure, como una máquina virtual, una cuenta de almacenamiento de Azure o una instancia de Virtual Machine Scale Sets. Un destino también puede ser un área de trabajo de Log Analytics o un recurso de Azure Application Insights. Para determinados recursos (por ejemplo, Azure Virtual Machines), puede especificar varios recursos como el destino de la regla de alerta.
* El recurso de destino de la alerta emite una **señal** en función del tipo de recurso seleccionado. La señal emitida puede ser *Métrica*, *Registro de actividad*, *Application Insights* o *Registro*.
* Define **criterios** para la regla de alerta que combinan la señal con la lógica de procesamiento. Los criterios se aplican al recurso de destino. Una combinación de criterios de ejemplo es \\* Percentage CPU &gt; 70%; Server Response Time &gt; 4 ms; and Result count of a log query &gt; 100.
* Puede especificar el nivel de **gravedad** de la regla de alerta que corresponde al problema relacionado con la alerta. La gravedad puede estar en el intervalo de 0 a 4.
* Cuando un problema coincide con las condiciones de la regla, el sistema invoca las **acciones** de la regla de alerta. Las acciones son los pasos con capacidad de respuesta que están relacionados con el problema, como el envío de notificaciones.
* De manera predeterminada, el sistema establece una regla de alerta nueva en *habilitada*. Si no desea que se desencadene una alerta, establezca la regla de alerta en *deshabilitada*.
* Una alerta solo se puede desencadenar cuando la regla de alerta está en estado *habilitado*.

**Creación de grupos de acciones**

Un grupo de acciones es una colección de preferencias de notificación que define como propietario de la suscripción de Azure. Cuando Azure Monitor detecta un problema en los datos de telemetría, se desencadena la alerta y se inician las acciones de regla de alerta. Azure Monitor, Azure Service Health y Azure Advisor usan *grupos de acciones* para notificar a los usuarios que se ha desencadenado una alerta.

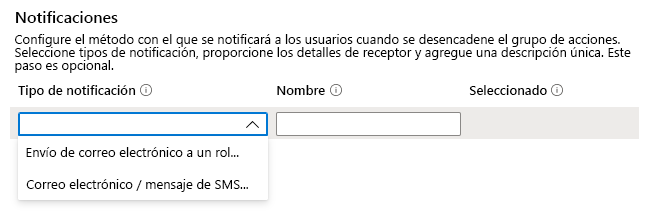
**Aspectos que debe saber sobre los grupos de acciones**

Vamos a revisar las características de los grupos de acciones, incluido cómo configurar las notificaciones y definir acciones.

* Múltiples alertas pueden usar el mismo grupo de acciones o distintos grupos de acciones en función de los requisitos del usuario.
* Las notificaciones especifican cómo notificar a los usuarios cuándo se desencadena el grupo de acciones.
* Las acciones especifican cómo invocar las acciones definidas cuando se desencadena el grupo de acciones.

**Notificaciones**

Puede configurar las notificaciones para que funcionen configurando el correo electrónico u opciones de comunicación similares.

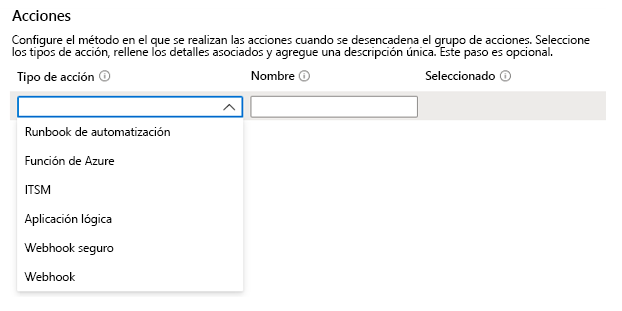


En Azure Portal, puede seleccionar la opción **Rol de Azure Resource Manager de correo electrónico** para enviar notificaciones por correo electrónico a los miembros del rol de la suscripción de Azure. El sistema envía correo electrónico solo a los miembros de usuario de Microsoft Entra del rol y no a grupos o entidades de servicio de Microsoft Entra.

También puede seleccionar la opción **Correo electrónico/SMS/Notificación de inserción/Voz** para especificar cualquier acción de correo electrónico, SMS, inserción o voz.

**Acciones**

Proporcione cada acción con un nombre y detalles únicos y defina las notificaciones o acciones que se van a realizar. Puede especificar acciones para enviar una llamada de voz, un mensaje SMS o un mensaje de correo electrónico.



Puede configurar el grupo de acciones para que use una acción automatizada mediante el atributo **Tipo de acción**. Estas son algunas opciones automatizadas:

* **Runbook de automatización**: un runbook de automatización permite definir, compilar, organizar y administrar flujos de trabajo que admiten procesos operativos de soporte y sistema, así como informar sobre ellos. Un flujo de trabajo de runbook puede llegar a interactuar con todos los tipos de elementos de infraestructura, como aplicaciones, bases de datos y hardware.
* **Azure Functions:** Azure Functions es un servicio de proceso sin servidor que le permite ejecutar código desencadenado por eventos sin tener que aprovisionar o administrar explícitamente la infraestructura.
* **ITSM:**: la acción permite conectar Azure y un producto o servicio compatible de Administración de servicios de TI (ITSM). Esta acción requiere una conexión de ITSM.
* **Logic Apps:**: Azure Logic Apps conecta las aplicaciones y los servicios críticos para la empresa mediante la automatización de los flujos de trabajo.
* **Webhook**: un webhook es un punto de conexión HTTPS o HTTP que permite a las aplicaciones externas comunicarse con el sistema.

**Comprobación de conocimiento**

Su empresa usa Azure Monitor para sus aplicaciones comerciales basadas en la nube en Azure. Está configurando notificaciones y alertas para asegurarse de que el equipo adecuado puede tomar medidas inmediatas para dar soporte a los clientes. Algunos equipos han enviado sus requisitos de configuración y sus preguntas para que los evalúe:

* El equipo de TI necesita un resumen de los tipos de alerta y las opciones de estado.
* El departamento de atención al cliente ha solicitado acciones de alerta automatizadas para resolver rápidamente los problemas del sitio web.
* La aplicación de búsqueda de inventario se utiliza todos los días de la semana. Un alto rendimiento de la aplicación es fundamental para admitir las operaciones diarias.

**Responda a las siguientes preguntas**

Elija la respuesta más adecuada para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

Principio del formulario

**1. ¿Qué indica una alerta en el estado *Confirmado*?**

1. El problema es nuevo (está abierto) y no está en revisión.
2. El problema está en revisión y el trabajo está en curso.
3. El problema se ha completado.

**2. ¿Qué característica de Azure Monitor puede notificar a los administradores en tiempo real los problemas críticos de la aplicación?**

1. Registros de actividad en Azure Monitor
2. Equipos de alertas
3. Grupos de acciones

**3. ¿De cuáles de los siguientes elementos consta una regla de alertas?**

1. Recursos, condiciones, acciones y detalles de alertas.
2. Recurso, condición, registro y tipo de alerta.
3. Métricas, registros, aplicación y sistema operativo.
4. B
5. C
6. A

Final del formulario

**Resumen y recursos**

En este módulo, obtuvo información sobre las alertas de Azure Monitor. Puede usar alertas para identificar y solucionar problemas antes de que afecten a los usuarios. Aprendió a configurar reglas de alertas de Azure basadas en señales de telemetría. Aprendió a configurar grupos de acciones para recibir notificaciones de alerta.

Las principales conclusiones de este módulo son:

* Azure Monitor captura datos de telemetría. Las alertas pueden usar estos datos para identificar y, a continuación, notificarle sobre posibles problemas.
* Hay diferentes tipos de alertas para admitir diversos escenarios de configuración y supervisión. Los tipos de alertas incluyen alertas de métricas, alertas de registro, alertas de registro de actividad y alertas de detección inteligente.
* Las alertas se administran supervisando el estado de la alerta. Los estados que se incluyen son: nueva, confirmada y cerrada.
* Las reglas de alerta se configuran en función del recurso de destino, la señal, los criterios y la gravedad.
* Los grupos de acciones definen las preferencias y acciones de notificación para cuando se desencadena una alerta. Estas acciones incluyen correo electrónico, SMS, inserción, llamadas de voz y acciones automatizadas.