**Introducción**

Azure Monitor recopila datos de registro y los almacena en tablas. Los administradores usan Log Analytics en Azure Portal para configurar sus orígenes de datos de entrada y realizar consultas de sus registros de Azure Monitor.

Las consultas proporcionan información sobre la infraestructura del sistema, como evaluar las actualizaciones del sistema y solucionar problemas de incidentes operativos. Para recuperar y consolidar los datos del repositorio, los administradores pueden crear consultas en el Lenguaje de consulta Kusto (KQL).

En este módulo, supongamos que es miembro de un equipo de administradores. Es responsable de comprender cómo trabajar con Azure Monitor y Log Analytics para implementar consultas y evaluar los datos de registro.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Identificar las características y los casos de uso de Log Analytics en Azure Monitor.
* Creación de un área de trabajo de Log Analytics en Azure Portal
* Usar KQL para estructurar una consulta de Log Analytics y revisar los resultados.

**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). En el módulo se tratan los siguientes requisitos de concepto de curso:

Supervisión y copia de seguridad de los recursos de Azure (10-15 %)

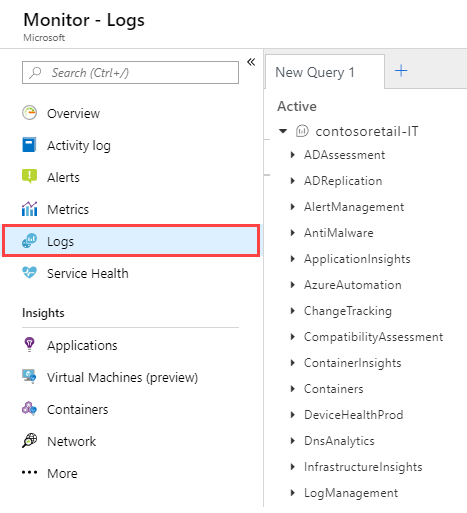
* Consulta y análisis de registros

**Requisitos previos**

Ninguno.

**Determinación de los usos de Log Analytics**

Log Analytics es una herramienta para Azure Monitor que está disponible en Azure Portal. Puede usar Log Analytics en Azure Monitor para editar y ejecutar consultas de registro con los datos recopilados en Azure Monitor. Las consultas de registro le ayudan a buscar patrones e identificar problemas.



**Aspectos que se deben saber sobre Log Analytics**

Vamos a examinar algunas características de Log Analytics en Azure Monitor.

* Log Analytics en Azure Monitor ofrece características y herramientas de consulta que le ayudan a responder prácticamente cualquier pregunta sobre la configuración supervisada.
* Log Analytics admite el Lenguaje de consulta Kusto (KQL). Puede crear consultas simples o complejas con KQL, entre las que se incluyen:
  + Buscar y ordenar por valor, hora, estado de propiedad, etc.
  + Combinar datos de varias tablas.
  + Agregar grandes conjuntos de datos.
  + Realizar operaciones complejas con código mínimo.
* Cuando los registros de Azure Monitor contienen datos recopilados suficientes y sabe cómo construir la consulta adecuada, puede usar Log Analytics para realizar análisis detallados y resolver problemas.

**Aspectos que se deben tener en cuenta al usar Log Analytics**

Algunas características de Azure Monitor, como conclusiones y soluciones, procesan los datos de registro sin exponer las consultas subyacentes. Para usar otras características de Azure Monitor, debe comprender cómo construir las consultas y aplicarlas para analizar de forma interactiva los datos en los registros de Azure Monitor. En los siguientes escenarios empresariales se muestran las ventajas de consultar los registros de Azure Monitor con Log Analytics.

**Escenario empresarial: Evaluación de los requisitos de actualización y el tiempo de finalización**

Una tarea diaria importante para los administradores de TI es evaluar los requisitos de actualización del sistema y planear las revisiones de configuración. Puesto que el proceso de aplicación de revisiones se relaciona con los Acuerdos de Nivel de Servicio de la empresa y puede afectar negativamente a las funciones empresariales, una programación precisa es fundamental.

En el pasado, los administradores tenían que programar una actualización de revisiones sin conocer muy bien el tiempo que tarda en completarse el proceso. Con una suscripción de Azure, los administradores pueden acceder a las ventajas de la plataforma Microsoft Azure. Azure recopila datos de todos los clientes que realizan revisiones. Azure usa los datos recopilados para proporcionar un tiempo medio de aplicación de revisiones para actualizaciones específicas.

Este uso de datos de "colaboración abierta distribuida" es único para los sistemas en la nube. Es un buen ejemplo de cómo Log Analytics en Azure Monitor puede ayudarle a cumplir los Acuerdos de Nivel de Servicio estrictos de su empresa.

**Escenario empresarial: Seguimiento de cambios e identificación de problemas de acceso**

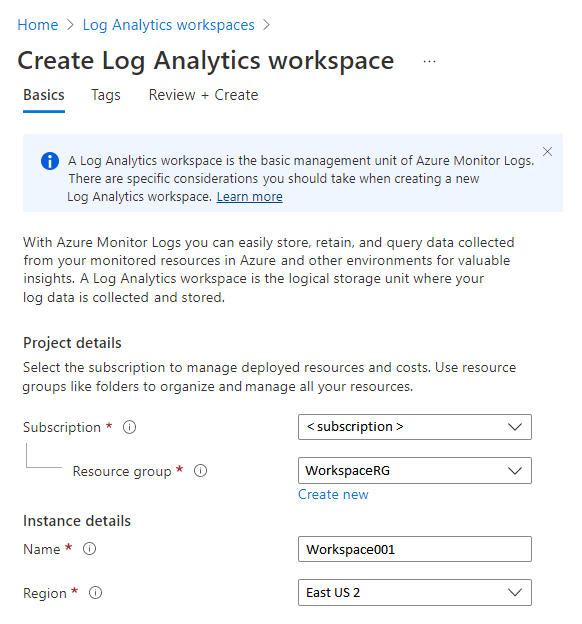
La solución de problemas de un incidente operativo es un proceso complejo que requiere acceso a varios flujos de datos. Mediante la supervisión de los sistemas desde la plataforma Azure, puede realizar análisis fácilmente desde varios ángulos. Tiene acceso a los datos de una amplia variedad de orígenes mediante una única interfaz para la correlación de información.

Mediante el seguimiento de los cambios en el entorno de Azure, Log Analytics de Azure Monitor puede ayudarle a identificar fácilmente problemas comunes, como:

* Comportamiento anómalo de una cuenta específica
* Usuarios que instalan software no aprobado
* Reinicios o apagados inesperados del sistema
* Evidencia de infracciones de seguridad
* Problemas específicos en aplicaciones de acoplamiento flexible

**Creación de un área de trabajo de Log Analytics**

Al capturar registros y datos en Azure Monitor, Azure almacena la información recopilada en un área de trabajo de Log Analytics. El área de trabajo de Log Analytics es el entorno de administración básico para los registros de Azure Monitor.



**Aspectos que se deben conocer sobre el área de trabajo de Log Analytics**

Para empezar a trabajar con Log Analytics en Azure Monitor, debe crear el área de trabajo. Un área de trabajo tiene un identificador de área de trabajo y un identificador de recurso únicos. Después de crear el área de trabajo, configure los orígenes de datos y las soluciones para almacenar sus datos en el área de trabajo.

Para crear el área de trabajo de Log Analytics, configure los parámetros siguientes:

* **Nombre**: proporcione el nombre de la nueva área de trabajo de Log Analytics. El nombre del área de trabajo debe ser único dentro del grupo de recursos.
* **Suscripción**: especifique la suscripción de Azure que se va a asociar al área de trabajo.
* **Grupo de recursos**: especifique el grupo de recursos que se va a asociar al área de trabajo. Puede elegir un grupo de recursos existente o crear uno. El grupo de recursos debe contener al menos una instancia de Azure Virtual Machines.
* **Región**: seleccione la región donde se crearon las máquinas virtuales.

**Nota**

La región debe admitir Log Analytics. Puede revisar las [**regiones que admiten Log Analytics**](https://azure.microsoft.com/explore/global-infrastructure/products-by-region/). En el cuadro **Buscar un producto**, escriba "Azure Monitor".

* **Precios**: el plan de tarifa predeterminado para una nueva área de trabajo es de *pago por uso*. Solo se aplican cargos después de empezar a recopilar datos.

Cada área de trabajo de Log Analytics en Azure Monitor puede tener un plan de tarifa diferente. Puede cambiar el plan de tarifa de un área de trabajo y realizar también un seguimiento de los cambios.

**Creación de consultas Kusto (KQL)**

Log Analytics en Azure Monitor admite el Lenguaje de consulta Kusto (KQL). La sintaxis de KQL le ayuda a crear consultas sencillas o complejas de forma rápida y fácil para recuperar y consolidar los datos de supervisión en el repositorio.

**Escritura de consultas de registro de KQL para Azure Monitor**

Vea el vídeo siguiente para aprender a escribir consultas de registro de KQL con Log Analytics en Azure Monitor. En el vídeo se tratan los siguientes conceptos:

* Visualización de datos de tabla en el repositorio de registros de Azure Monitor
* Creación de consultas sencillas y complejas
* Filtrado y resumen de los resultados de búsqueda
* Adición de visualizaciones a los resultados de búsqueda

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

<https://youtu.be/cAzlAg2L1Bg>

En la unidad siguiente, veremos más detenidamente cómo estructurar una consulta KQL.

**Aspectos que se deben tener en cuenta al usar consultas KQL**

Estas son algunas de las muchas cosas que puede realizar con las consultas de registro de KQL en Log Analytics:

*Crear y guardar búsquedas de los datos almacenados en el repositorio de registros de Azure Monitor*.

*Usar las búsquedas de registros guardadas para analizar directamente los datos en Azure Portal*.

*Configurar las búsquedas de registros guardadas para que se ejecuten automáticamente*.

*Configurar las búsquedas de registros guardadas para generar alertas de notificación*.

*Agregar visualizaciones a las búsquedas de registros guardadas para obtener vistas gráficas del estado del entorno*.

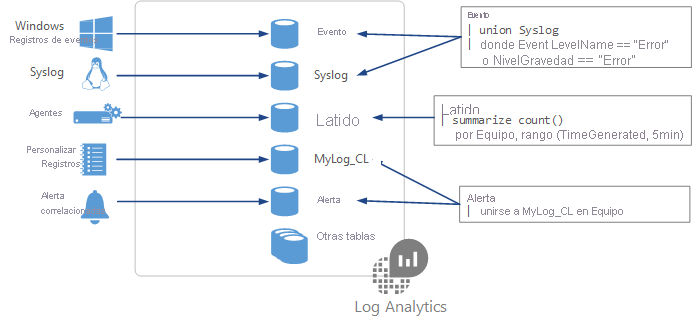
*Exportar los datos del repositorio a herramientas como Power BI o Excel para analizar los datos fuera de Log Analytics*.

*Crear soluciones de consulta personalizadas con la*[*API REST de Log Analytics*](https://learn.microsoft.com/es-es/rest/api/loganalytics/).

**Estructuración de las consultas de Log Analytics**

Los administradores crean consultas de Log Analytics a partir de los datos almacenados en tablas dedicadas en un área de trabajo de Log Analytics. Algunas tablas de consulta comunes son Evento, Syslog, Latido y Alerta. Al compilar una consulta de Lenguaje de consulta Kusto (KQL), empiece por determinar qué tablas del repositorio de registros de Azure Monitor tienen los datos que busca.

En la ilustración siguiente se resalta cómo las consultas KQL usan los datos de la tabla dedicada en los servicios y recursos supervisados.



**Aspectos que se deben conocer sobre la estructura de las consultas KQL**

Echemos un vistazo más de cerca a los datos de tablas dedicadas y cómo estructurar una consulta de registro de KQL.

* Cada origen de datos y solución seleccionados almacena sus datos en tablas dedicadas en el área de trabajo de Log Analytics.
* La documentación de cada origen de datos y solución incluye el nombre del tipo de datos que crea y una descripción de cada una de sus propiedades.
* La estructura básica de una consulta es una tabla de origen seguida de una serie de comandos (conocidos como *operadores*).
* Una consulta puede tener una cadena de varios operadores para refinar los datos y realizar funciones avanzadas.
* Cada operador de una cadena de consulta comienza con un carácter de barra vertical |.
* Muchas consultas solo necesitan datos de una tabla, pero otras pueden usar diversas opciones e incluir datos de varias tablas.

**Ejemplos de consultas de registro de KQL**

Vamos a revisar algunos operadores de consulta de registro de KQL comunes y sintaxis de ejemplo.

Podemos crear consultas para buscar datos en la tabla StormEvent que tiene cinco entradas:

| **type** | **event** | **severity** | **start** | **duration** | **region** |
| --- | --- | --- | --- | --- | --- |
| Water | Freezing rain | 1 | 6:00 AM 01-27-2023 | 3 hours | 1, 2 |
| Wind | High winds | 1 | 8:00 AM 01-27-2023 | 12 hours | 1, 2, 4, 5 |
| Temperature | Below freezing | 2 | 11:00 PM 01-26-2023 | 10 hours | 1, 2, 4, 5 |
| Water | Snow | 3 | 4:00 PM 01-26-2023 | 10 hours | 1, 2, 4, 5 |
| Water | Flood warning | 2 | 9:00 AM 01-26-2023 | 10 hours | 3 |

Para buscar otros operadores y ejemplos, consulte [Consultas de registro de Azure Monitor](https://learn.microsoft.com/es-es/azure/azure-monitor/log-query/query-language).

**Número de elementos de recuento**

Use el operador count para detectar el número de registros de un conjunto de registros de entrada.

En el ejemplo siguiente se devuelve el número de registros de la tabla StormEvent. Los resultados de la consulta revelan que la tabla StormEvent tiene cinco entradas.

StormEvent | count

Resultados de la consulta:

| **count** |
| --- |
| 5 |

**Devolver el primer número de elementos**

Use el operador top para ver los primeros N registros del conjunto de registros de entrada, ordenados por las columnas especificadas. Las columnas corresponden a las propiedades de datos definidas en la tabla dedicada.

En el ejemplo siguiente se devuelven los tres primeros registros de datos de StormEvent. La tabla de resultados muestra el nombre event de la tormenta, la gravedad y la duración prevista.

StormEvent | top 3 by event severity duration

Resultados de la consulta:

| **event** | **severity** | **duration** |
| --- | --- | --- |
| Freezing rain | 1 | 3 hours |
| High winds | 1 | 12 hours |
| Below freezing | 2 | 10 hours |

**Buscar elementos coincidentes**

Use el operador where para filtrar la tabla por el subconjunto de filas que coinciden con el valor de predicado proporcionado. El valor de predicado indica qué buscar en la tabla, como en where=="find-this".

En el ejemplo siguiente se filtran los registros de datos de StormEvent para que solo se usen los registros que coincidan con "snow".

StormEvent | where event=="snow"

La consulta filtra por una fila de la tabla StormEvent:

| **type** | **event** | **severity** | **start** | **duration** | **region** |
| --- | --- | --- | --- | --- | --- |
| Water | Snow | 3 | 4:00 PM 01-26-2023 | 10 hours | 1, 2, 4, 5 |

**Agregar contenido**

Use el operador summarize para crear una tabla que agregue el contenido del conjunto de registros de entrada en función de las especificaciones.

En el ejemplo siguiente se devuelve una tabla agregada para StormEvent. La tabla de resultados muestra el nivel de gravedad promedio (avg) de cada tipo de tormenta en cada region de todos los registros de datos (count) de la tabla dedicada.

StormEvent | summarize count(), avg(severity) by type, region

Resultados de la consulta:

| **type** | **avg(severity)** | **region** |
| --- | --- | --- |
| Water | 2 | 1, 2, 3 |
| Water | 3 | 4, 5 |
| Wind | 1 | 1, 2, 4, 5 |
| Temperature | 2 | 1, 2, 4, 5 |

**Operadores de cadena**

Cualquier consulta puede contener una cadena de operadores.

Supongamos que quiere buscar en la tabla StormEvent cuántos días han tenido temperaturas bajo cero en las dos últimas semanas. Si hay resultados, querrá verlos en orden descendente (la fecha más antigua primero).

Puede crear una consulta con operadores encadenados: where y summarize. La consulta busca en los datos de tabla recopilados en los últimos ago(14days). Busca coincidencias con la cadena Below, que forma parte del texto de entrada Below freezing del tipo de tormenta Temperature.

La tabla de resultados agrega (summarize) todos los elementos (count) de la tabla dedicada y muestra los elementos devueltos en orden descendente (desc).

StormEvent

| where (EventLevelName == "Below")

| where (TimeGenerated > ago(14days))

| summarize StormEvent = count(), desc

Resultados de la consulta:

| **type** | **event** | **start** |
| --- | --- | --- |
| Temperature | Below freezing | 11:00 PM 01-13-2023 |
| Temperature | Below freezing | 12:00 AM 01-14-2023 |
| Temperature | Below freezing | 3:00 AM 01-16-2023 |
| Temperature | Below freezing | 12:00 AM 01-17-2023 |
| Temperature | Below freezing | 11:00 PM 01-26-2023 |

**Prueba de conocimientos**

Su empresa opera una granja de servidores web de gran tamaño con más de 100 máquinas virtuales. Han decidido usar Log Analytics en Azure Monitor para configurar sus orígenes de datos de entrada. Está desarrollando consultas con el Lenguaje de consulta Kusto (KQL) para filtrar y evaluar los datos de registro de la máquina virtual. Estas son algunas de las tareas y consideraciones que debe abordar:

* Necesita una consulta compleja para supervisar los registros de la máquina virtual y ver los datos en distintos modelos.
* Está investigando escenarios para usar agentes de Log Analytics.
* El equipo del sitio web ha solicitado un resumen de las opciones para organizar los datos de registro en Azure Monitor.

**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. ¿Cómo organiza Azure Monitor los datos de registro?**

1. Colas de eventos
2. Archivos de texto
3. Tablas

**2. ¿Qué comandos de KQL crean una agregación de datos de entrada y generan objetos visuales para los resultados de la consulta?**

1. summarize y render
2. aggregate y visualize
3. count y project

**3. ¿Qué recurso pueden ejecutar los agentes de Log Analytics?**

1. Solo en equipos en la nube.
2. En varias plataformas, incluidos otros proveedores de nube.
3. Solo en equipos físicos.
4. C
5. A
6. B

Final del formulario

**Resumen y recursos**

Los administradores de Azure trabajan con Log Analytics en Azure Portal para ejecutar consultas de registro en sus datos en los registros de Azure Monitor. Los administradores pueden crear consultas de Lenguaje de consulta Kusto (KQL) para consolidar y analizar sus datos.

En este módulo, ha identificado las características y los casos de uso de Log Analytics en Azure Monitor. Ha creado un área de trabajo de Log Analytics en Azure Portal. Ha revisado cómo usar KQL para estructurar una consulta de Log Analytics y revisar los resultados.