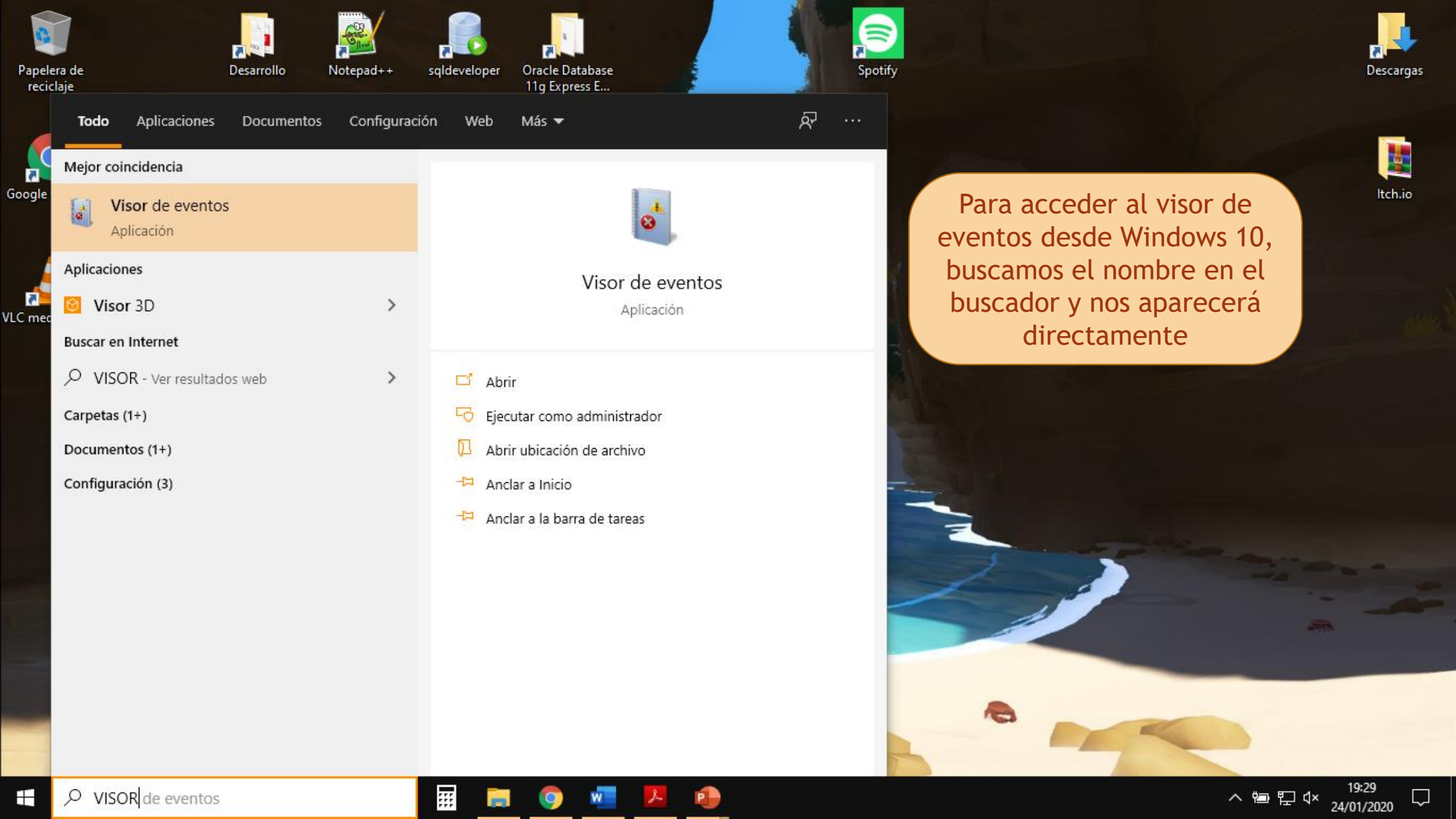


6.1. Herramientas avanzadas en Windows (II).Visor de eventos

Álvaro Cañizares
DA1D1E

SISTEMAS INFORMÁTICOS



Para acceder al visor de eventos desde Windows 10, buscamos el nombre en el buscador y nos aparecerá directamente

Todo Aplicaciones Documentos Configuración Web Más

Mejor coincidencia

 **Visor de eventos**
Aplicación

Aplicaciones

 **Visor 3D**

Buscar en Internet

 VISOR - Ver resultados web






Carpetas (1+)

Documentos (1+)

Configuración (3)

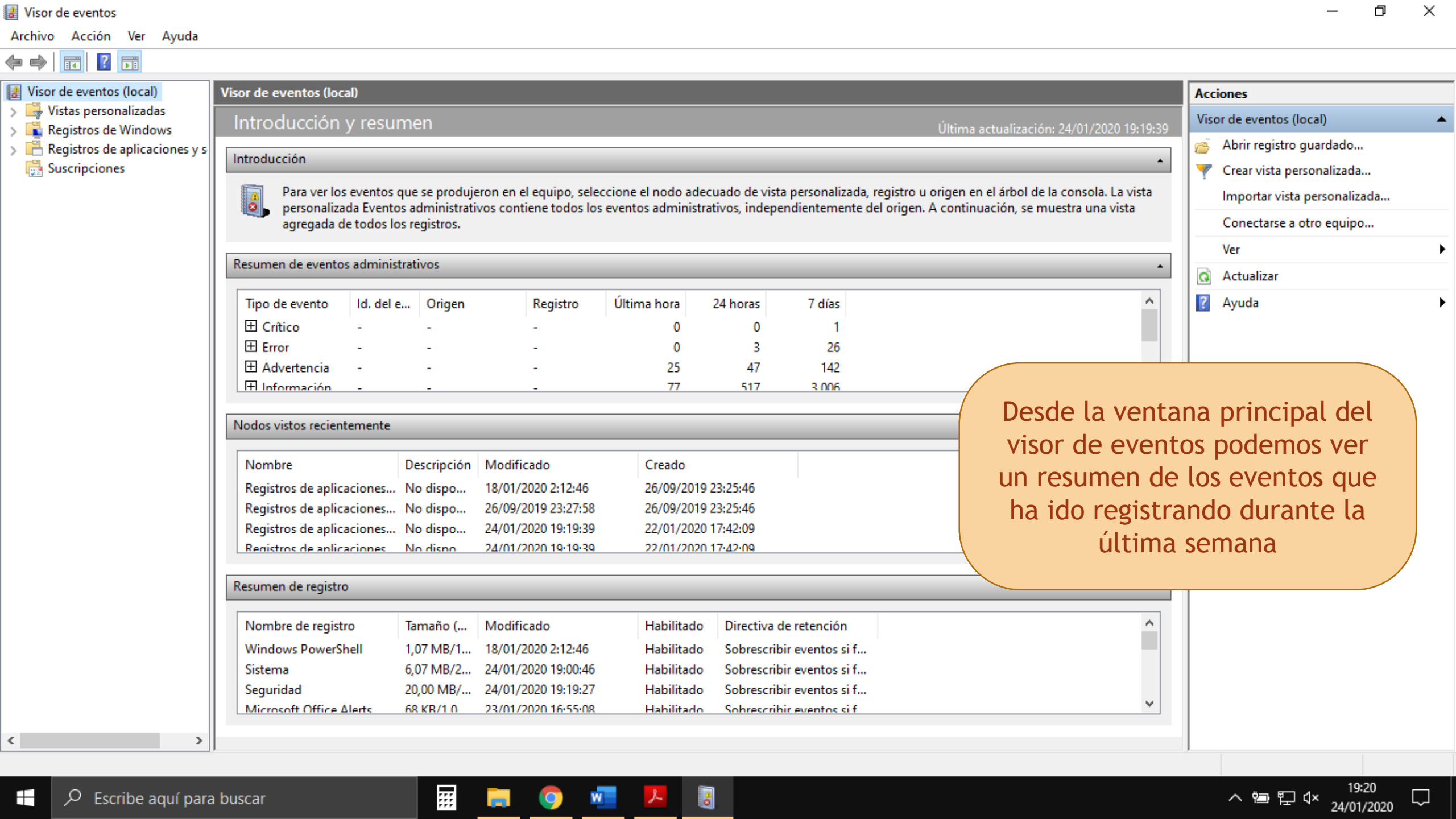


Visor de eventos
Aplicación

-  Abrir
-  Ejecutar como administrador
-  Abrir ubicación de archivo
-  Anclar a Inicio
-  Anclar a la barra de tareas

VISOR|de eventos

19:29
24/01/2020



Visor de eventos (local)

Introducción y resumen

Última actualización: 24/01/2020 19:19:39

Introducción



Para ver los eventos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el árbol de la consola. La vista personalizada Eventos administrativos contiene todos los eventos administrativos, independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.

Resumen de eventos administrativos

Tipo de evento	Id. del e...	Origen	Registro	Última hora	24 horas	7 días
⊕ Crítico	-	-	-	0	0	1
⊕ Error	-	-	-	0	3	26
⊕ Advertencia	-	-	-	25	47	142
⊕ Información	-	-	-	77	517	3.006

Nodos vistos recientemente

Nombre	Descripción	Modificado	Creado
Registros de aplicaciones...	No dispo...	18/01/2020 2:12:46	26/09/2019 23:25:46
Registros de aplicaciones...	No dispo...	26/09/2019 23:27:58	26/09/2019 23:25:46
Registros de aplicaciones...	No dispo...	24/01/2020 19:19:39	22/01/2020 17:42:09
Registros de aplicaciones...	No dispo...	24/01/2020 19:19:39	22/01/2020 17:42:09

Resumen de registro

Nombre de registro	Tamaño (...)	Modificado	Habilitado	Directiva de retención
Windows PowerShell	1,07 MB/1...	18/01/2020 2:12:46	Habilitado	Sobrescribir eventos si f...
Sistema	6,07 MB/2...	24/01/2020 19:00:46	Habilitado	Sobrescribir eventos si f...
Seguridad	20,00 MB/...	24/01/2020 19:19:27	Habilitado	Sobrescribir eventos si f...
Microsoft Office Alerts	68 KB/1 0	23/01/2020 16:55:08	Habilitado	Sobrescribir eventos si f...

Acciones

Visor de eventos (local)

- Ⓜ Abrir registro guardado...
- 🔍 Crear vista personalizada...
- 📁 Importar vista personalizada...
- 🔌 Conectarse a otro equipo...
- Ver
- 🔄 Actualizar
- 🔍 Ayuda

Desde la ventana principal del visor de eventos podemos ver un resumen de los eventos que ha ido registrando durante la última semana

Visor de eventos

ArchivoAcciónVerAyuda

Visor de eventos (local)

Vistas personalizadas

Registros de Windows

Aplicación

Seguridad

Instalación

Sistema

Eventos reenviados


Registros de aplicaciones y suscripciones

Visor de eventos (local)

Introducción y resumen

Última actualización: 24/01/2020 19:19:39

Introducción



Para ver los eventos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el árbol de la consola. La vista personalizada Eventos administrativos contiene todos los eventos administrativos, independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.

Resumen de eventos administrativos

Tipo de evento	Id. del e...	Origen	Registro	Última hora	24 horas	7 días
Error	-	-	-	0	3	26
	0	Office 2016 Licensing Service	Aplicación	0	0	1
	2	Kernel-EventTracing	Microsoft...	0	0	1
	3	Kernel-EventTracing	Microsoft	0	1	8

Nodos vistos recientemente

Nombre	Descripción	Modificado	Creado
Registros de aplicaciones...	No dispo...	18/01/2020 2:12:46	26/09/2019 23:25:46
Registros de aplicaciones...	No dispo...	26/09/2019 23:27:58	26/09/2019 23:25:46
Registros de aplicaciones...	No dispo...	24/01/2020 19:19:39	22/01/2020 17:42:09
Registros de aplicaciones...	No dispo...	24/01/2020 19:19:39	22/01/2020 17:42:09

Resumen de registro

Nombre de registro	Tamaño (...)	Modificado	Habilitado	Directiva de retención
Windows PowerShell	1,07 MB/1...	18/01/2020 2:12:46	Habilitado	Sobrescribir eventos si f...
Sistema	6,07 MB/2...	24/01/2020 19:00:46	Habilitado	Sobrescribir eventos si f...
Seguridad	20,00 MB/...	24/01/2020 19:19:27	Habilitado	Sobrescribir eventos si f...
Microsoft Office Alerts	68 KB/1 0	23/01/2020 16:55:08	Habilitado	Sobrescribir eventos si f...

Acciones

Visor de eventos (local)

Abrir registro guardado...

Crear vista personalizada...

Importar vista personalizada...

Conectarse a otro equipo...

Ver

Actualizar

Ayuda

Evento 0, Office 2016 Licensing Service

Ver todas las instancias de este eve...

Ayuda

En la carpeta de Registros de Windows podemos observar de manera más específica los eventos

Windows

Escribe aquí para buscar

Calculadora

Explorador de archivos

Google Chrome

Word

PDF

Visor de eventos

19:21

24/01/2020



- Visor de eventos (local)
- Vistas personalizadas
- Registros de Windows
 - Aplicación
 - Seguridad
 - Instalación
 - Sistema
 - Eventos reenviados
- Registros de aplicaciones y suscripciones

Sistema Número de eventos: 10.422

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Advertencia	24/01/2020 18:51:31	DNS Client Events	1014	(1014)
Información	24/01/2020 18:51:23	k57nd60a	9	Ninguno
Advertencia	24/01/2020 18:51:15	DNS Client Events	1014	(1014)
Advertencia	24/01/2020 18:51:12	k57nd60a	4	Ninguno
Información	24/01/2020 18:51:11	k57nd60a		
Advertencia	24/01/2020 18:51:09	k57nd60a		
Información	24/01/2020 18:51:08	k57nd60a		
Advertencia	24/01/2020 18:51:06	k57nd60a		
Información	24/01/2020 18:51:05	k57nd60a		
Advertencia	24/01/2020 18:50:54	k57nd60a		
Información	24/01/2020 18:50:53	k57nd60a		
Advertencia	24/01/2020 18:50:51	k57nd60a		
Información	24/01/2020 18:50:50	k57nd60a		
Advertencia	24/01/2020 18:50:48	k57nd60a		
Información	24/01/2020 18:50:47	k57nd60a		
Advertencia	24/01/2020 18:50:36	k57nd60a		
Información	24/01/2020 18:20:32	k57nd60a		

En este caso, la mayoría de errores se encuentran ubicados en la división de Sistema, para obtener los datos de este lo clicamos

Evento 1014, DNS Client Events

General Detalles

Se agotó el tiempo de espera para la resolución del nombre mtalk.google.com después de que ninguno de los servidores DNS configurados respondiese.

Nombre de registro:

Sistema

Origen:

DNS Client Events

Registrado:

24/01/2020 18:51:31

Id. del

1014

Categoría de tarea:

(1014)

Nivel:

Advertencia

Palabras clave:

(268435456)

Usuario:

Servicio de red

Equipo:

Tom

Acciones

- Sistema
 - Abrir registro guardado...
 - Crear vista personalizada...
 - Importar vista personalizada...
 - Vaciar registro...
 - Filtrar registro actual...
 - Propiedades
 - Buscar...
 - Guardar todos los eventos como...
 - Adjuntar tarea a este registro...
- Ver
 - Actualizar
 - Ayuda
- Evento 1014, DNS Client Events
 - Propiedades de evento
 - Adjuntar tarea a este evento...
 - Copiar
 - Guardar eventos seleccionados...
 - Actualizar
 - Ayuda

Visor de eventos

ArchivoAcciónVerAyuda

Visor de eventos (local)

Vistas personalizadas

Registros de Windows

Aplicación

Seguridad

Instalación

Sistema

Eventos reenviados

Registros de aplicaciones y servicios

Suscripciones

Sistema

Número de eventos: 10.422

Nivel	Fecha y hora	Origen	Id. del evento
Advertencia	24/01/2020 18:51:31	DNS Client Events	1014
Información	24/01/2020 18:51:23	k57nd60a	9
Advertencia	24/01/2020 18:51:15	DNS Client Events	1014

Propiedades de evento: Evento 1014, DNS Client Events

General

Detalles

Se agotó el tiempo de espera para la resolución del nombre mtalk.google.com después de que ninguno de los servidores DNS configurados respondiese.

Nombre de registro: Sistema

Origen: DNS Client Events

Id. del: 1014

Nivel: Advertencia

Usuario: Servicio de red

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

Registrado: 24/01/2020 18:51:31

Categoría de tarea: (1014)

Palabras clave: (268435456)

Equipo: Tom

Copiar

Cerrar

Buscar...

Guardar todos los eventos como...

Adjuntar tarea a este registro...

Ver

Actualizar

Ayuda

Evento 1014, DNS Client Events

Propiedades de evento

Adjuntar tarea a este evento...

Copiar

Guardar eventos seleccionados...

Actualizar

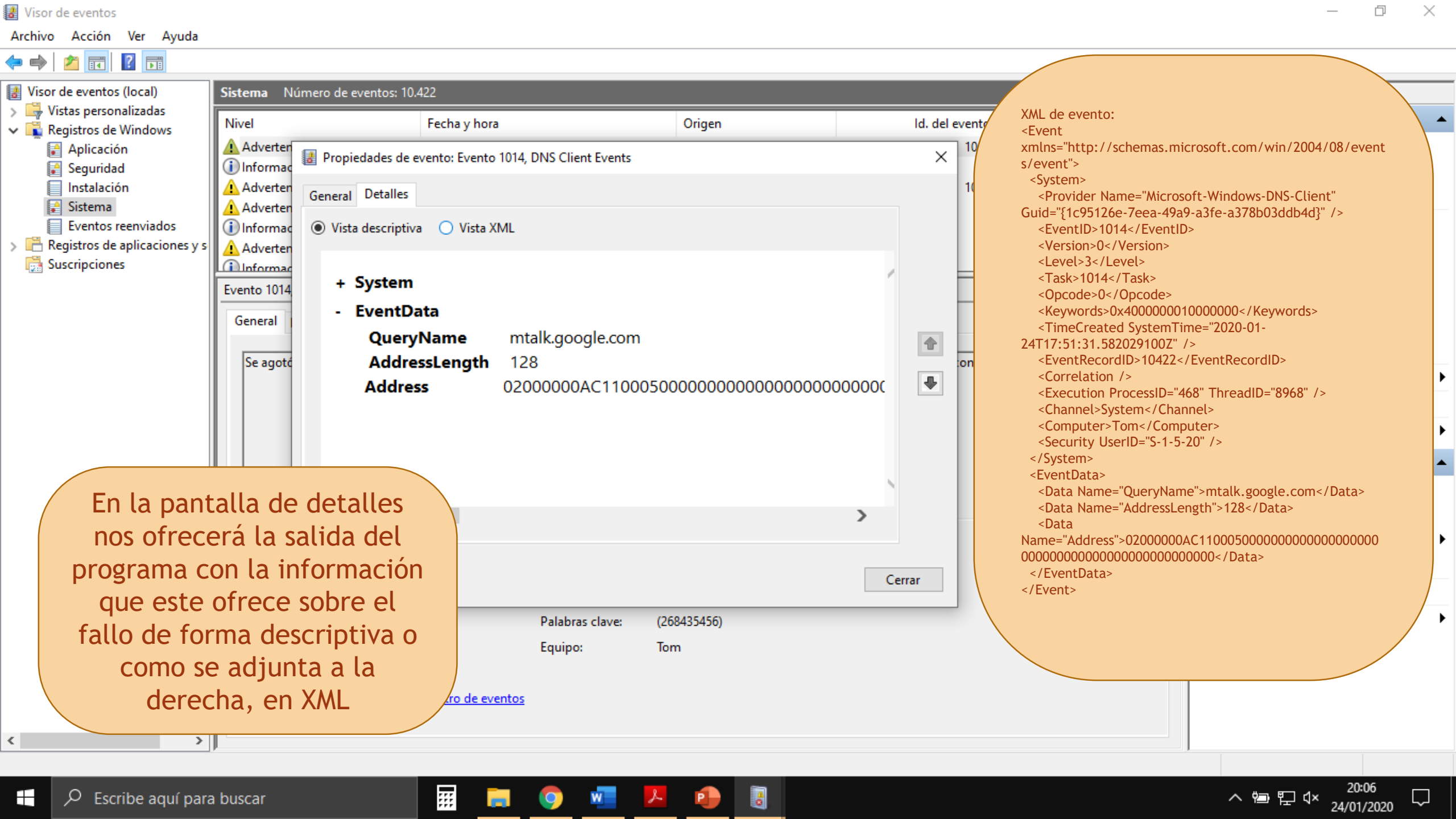
Ayuda

Desde la pestaña general observamos la descripción que hace el evento del error, así como una serie de datos sobre el registro de este evento

Escribe aquí para buscar

19:22

24/01/2020



En la pantalla de detalles nos ofrecerá la salida del programa con la información que este ofrece sobre el fallo de forma descriptiva o como se adjunta a la derecha, en XML

XML de evento:

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/event
s/event">
  <System>
    <Provider Name="Microsoft-Windows-DNS-Client"
Guid="{1c95126e-7eea-49a9-a3fe-a378b03ddb4d}" />
    <EventID>1014</EventID>
    <Version>0</Version>
    <Level>3</Level>
    <Task>1014</Task>
    <Opcode>0</Opcode>
    <Keywords>0x4000000010000000</Keywords>
    <TimeCreated SystemTime="2020-01-
24T17:51:31.582029100Z" />
    <EventRecordID>10422</EventRecordID>
    <Correlation />
    <Execution ProcessID="468" ThreadID="8968" />
    <Channel>System</Channel>
    <Computer>Tom</Computer>
    <Security UserID="S-1-5-20" />
  </System>
  <EventData>
    <Data Name="QueryName">mtalk.google.com</Data>
    <Data Name="AddressLength">128</Data>
    <Data
Name="Address">02000000AC11000500000000000000000000000000
00000000000000000000000000000000</Data>
  </EventData>
</Event>
```

FIN