SYSLOG - Qué es en realidad y qué significa

Artículo
Mario Sanchez Macias · Sep 26, 2019 Lectura de 8 min

SYSLOG - Qué es en realidad y qué significa

¡Hola a todos!

En esta publicación me gustaría hablar sobre la tabla syslog: qué es, cómo analizarla, cuáles son realmente las entradas y por qué puede ser importante para usted. La tabla syslog puede contener información de diagnóstico importante. Si su sistema tiene algún problema, es importante entender cómo analizar esta tabla y qué información contiene.

¿Qué es una tabla syslog?

Caché reserva una pequeña porción de su memoria compartida para registrar elementos importantes. Esta tabla tiene varios nombres diferentes:

- errlog
- SYSLOG
- tabla syslog

Para cumplir con el propósito de esta publicación, simplemente la llamaré 'tabla syslog'.

El tamaño de la tabla syslog puede configurarse. El valor predeterminado es de 500 entradas. El intervalo es de 10 a 10,000 entradas. Para cambiar el tamaño de la tabla syslog ve al Portal de administración y entra en Administración -> Configuración -> Configuración adicional-> Memoria avanzada y en la fila ‘errlog’ selecciona ‘editar’ e introduce el número de entradas deseado para la tabla syslog.

¿Por qué se quiere cambiar el tamaño de la tabla syslog?

Si la tabla syslog se configura para 500 entradas, en la entrada 501 se sobrescribirá la primera entrada, y esa información se perderá. Esta tabla se encuentra en la memoria y por lo tanto no persiste en ningún lugar, a menos que la salida se guarde de manera específica. Además, cuando se paré Caché, todas las entradas se perderán a menos que se configure para guardar las entradas en el archivo cconsole.log, como se describe a continuación.

Si Caché introduce muchas entradas en la tabla syslog, y necesitas analizarlas para ayudar a diagnosticar cualquier problema, se perderán las entradas si la tabla no es lo suficientemente grande. Puedes analizar la columna Fecha/Hora que se encuentra en la tabla de syslog para determinar el periodo de tiempo que lleva llenar la tabla. Esto te ayudará para decidir cuántas entradas necesitas. A mí me gusta tener controlada la tabla y aumentarla para no perder ninguna entrada.

¿Cómo puedo analizar la tabla syslog?

Existen varias maneras de analizar la tabla syslog:

1. Desde una línea de comandos en el terminal de Caché en el namespace %SYS, ‘Do ^SYSLOG’
2. Desde una línea de comandos en el terminal de Caché en el namespace %SYS, ‘do ^Buttons’
3. Desde el Portal web de administración : Operaciones -> Informes de diagnóstico
4. Ejecutando cstat con la opción -e1
5. Ejecutando Cachehung

6. Configurando Caché para volcar la tabla syslog en el archivo cconsole.log al apagar el sistema. Para hacer esto entra en el Portal de administración web y ve a Administración -> Configuración -> Configuración adicional -> Compatibilidad, en la fila 'ShutDownLogErrors', selecciona 'editar' y activa el check ('true') para guardar el contenido de syslog en cconsole.log cuando se paré Caché.

¿Qué significan las entradas de syslog?

A continuación, se muestra un ejemplo de la tabla syslog. Este ejemplo se origina de la ejecución de ^SYSLOG en la línea de comandos del terminal de Caché:

```
%SYS>d ^SYSLOG

Device:
Right margin: 80 =>
Show detail? No => No
Cache System Error Log printed on Nov 02 2016 at  4:29 PM
-----------------------------------------------------
Printing the last 8 entries out of 8 total occurrences.
Err  Process         Date/Time                          Mod     Line      Routine
                           Namespace
9     41681038     11/02/2016 04:44:51PM     93        5690     systest+3^systest
     %SYS
9     41681038     11/02/2016 04:43:34PM     93        5690     systest+3^systest
     %SYS
9     41681038     11/02/2016 04:42:06PM     93        5690     systest+3^systest
     %SYS
9     41681038     11/02/2016 04:41:21PM     93        5690     systest+3^systest
     %SYS
9     41681038     11/02/2016 04:39:29PM     93        5690     systest+3^systest
     %SYS
9     41681036     11/02/2016 04:38:26PM     93        5690     systest+3^systest
     %SYS
9     41681036     11/02/2016 04:36:57PM     93        5690     systest+3^systest
     %SYS
9     41681036     11/02/2016 04:29:45PM     93        5690     systest+3^systest
     %SYS
```

Puede parecer evidente, según los títulos de las columnas, el significado de cada uno de los elementos de una entrada, pero los describiré todos.

Printing the last 8 entries out of 8 total occurrences

Aunque esto no es parte de una entrada en la tabla syslog, es algo importante que se debe considerar, así que lo mencionaré. Aquí es donde se mira para encontrar cuántas entradas contiene la tabla syslog. En este ejemplo, solo se generaron 8 entradas desde que se inició Caché. Este es mi sistema de pruebas, así que tiene muchas entradas. Si aparece ‘Printing the last 500 entries out of 51234 total occurrences’ sabrás que se han perdido muchas entradas. En estos casos, aumenta el tamaño de la tabla hasta un máximo de 10,000 (si se está interesado en ver estas entradas) o ejecuta SYSLOG con mayor frecuencia.

Err

Esta es la información que registramos sobre el evento de interés. Normalmente suele ser un error a nivel del sistema operativo (SO), para encontrar qué error de SO se refiere tienes dos opciones:

- En Linux/Unix: los números de error se suelen encuentran en /usr/include/errno.h.
- En Windows pueden consultarse con `>net helpmsg <numero>`.

Pero no siempre es de SO y también podría ser cualquier otra cosa que necesitamos registrar. Por ejemplo, podría contener información de depuración para para un valor determinado de una variable interna o nuestros propios código de de error (cualquier cosa mayor a 10,000).

Pero ¿Cómo se puede saber qué es? Para saber qué es, debemos analizar la línea de código fuente que se indica mediante "mod" y "line". En la práctica, esto significa que no es posible encontrar ese detalle sin contactar a InterSystems. ¿Entonces, por qué molestarse en analizarlo? Bueno, existen muchas cosas que puede averiguar sin saber exactamente lo que es err, echando un vistazo a otro tipo de información. Además, puedas ponerte en contacto con InterSystems si ves que existen muchas entradas, o entradas diferentes a las entradas que normalmente ves en un sistema saludable.

Por otro lado, hay que tener también en cuenta que una entrada en la tabla syslog no siempre implica un error. (Pueden aparecer mensajes de desconexión, fichero no encontrado, etc... que no son realmente errores si están controlados).

Process

Este es el ID del proceso que introdujo la entrada en la tabla syslog. Por ejemplo, si tienes un proceso bloqueado, en loop o muerto, puedes analizar la tabla syslog para consultar si existe algún registro. Si lo hizo, probablemente será una pista importante de por qué el proceso tuvo problemas.

Date/Time

Esta es la fecha y la hora en que se realizó la entrada. Es muy importante correlacionar la fecha y la hora de la entrada con la de cualquier evento del sistema, porque con frecuencia es una pista de lo que salió mal.

Mod y Line

Mod corresponde a un archivo específico en C, y line es el número de línea en ese archivo que introdujo la entrada en la tabla syslog. Solo el personal de InterSystems que cuenta con acceso al código del kernel puede buscarlo. Solo buscando este código se puede saber exactamente lo que se registra en la entrada.

Routine

Las etiquetas, el offset y la rutina que el proceso estaba ejecutando cuando se llevo a cabo la entrada en la tabla syslog. Esto puede ayudar a averiguar lo que ocurre.

Namespace

Este es el namespace en el que se ejecutó el proceso.

Por tanto ¿cómo puedo determinar por qué err 9 está en mi tabla syslog?

Primero, analizamos la rutina indicada. Esta es la rutina ^systest del ejemplo anterior:

```
systest  ;test for syslog post
         s file="/home/testfile"
         o file:10
         u file w "hello world"
         c file
         q
```

La entrada de syslog indica que systest+3 es lo que se ejecutó cuando se llevo a cabo la entrada. Esta línea es:

```
u file w "hello world"
```

Dado que el proceso intentaba escribir en un archivo, esto podría ser un error a nivel de sistema operativo (OS),

así que buscamos el código de error 9 en /usr/include/errno.h y encontramos:

```
#define EBADF   9       /* Bad file descriptor                  */
```

Dado que 9 está relacionado con los archivos y la línea de código intenta escribir en un archivo, es razonable suponer que realmente se trata de un error en el código devuelto por el sistema operativo.

¿Podemos determinar qué está mal?

Para resolver esto, primero analizamos los permisos que se encuentran en el directorio /home y en el archivo de prueba. Ambos eran 777, así que realmente debió ser capaz de abrir y escribir en ese archivo. Al analizar más de cerca el código nos damos cuenta de un error. Antes de los dos puntos del tiempo de espera de diez segundos se necesita utilizar algunos parámetros en el comando open. A continuación, se muestra la rutina actualizada que realmente termina sin errores y se escribe en el archivo:

```
systest  ;test for syslog post
         s file="/scratch1/yrockstr/systest/testfile"
         o file:"WNSE":10
         u file w "hello world"
         c file
         q
```

Resumen

La tabla syslog es una herramienta valiosa para depurar si se utiliza correctamente. Hay que tener en cuenta lo siguiente cuando se utilice:

1. **err** no siempre es un error del sistema operativo. Pónte en contacto con InterSystems para conocer lo en detalle lo que se ha registrado.
2. Utiliza otros datos relacionados para determinar lo que sucede. La línea del código COS combinada con el error puede ofrecer una suposición razonable de si es un error del sistema operativo o nuestro código.
3. Realiza búsquedas en la tabla syslog cada vez que tengas un problema que no puedas resolver, es posible que la pista esté allí.
4. Utilice la Date/Time, el número de entradas y el total de sucesos para determinar si necesita aumentar el tamaño de su tabla de syslog
5. Conoce lo que tu sistema registra en la tabla syslog para controlar si se producen cambios o entradas nuevas o diferentes
6. Las entradas en la tabla syslog no necesariamente son un problema. El tenerlas controladas es la clave

#Consejos y trucos #Monitorización #Terminal #Caché
00 2 0 0 88

Log in or sign up to continue
Añade la respuesta

URL de fuente: https://es.community.intersystems.com/post/syslog-qu%C3%A9-es-en-realidad-y-qu%C3%A9-significa