

Artículo

[Mario Sanchez Macias](#) · Abr 27, 2021 · Lectura de 21 min

Plataformas de datos InterSystems y su rendimiento: Backups de VM y scripts de freeze/thaw de Caché

Esta publicación es la traducción de un artículo que publicó mi compañero Murray hace un tiempo. Durante mi trabajo en soporte la he recomendado muchas veces, pues lo que aquí se explica es bastante común y los ejemplos que se dan pueden ayudar a muchos de vosotros.

En esta publicación muestro estrategias para realizar copias de seguridad de Caché utilizando un Backup externo, con ejemplos de integración con soluciones basadas en snapshots. La mayoría de soluciones que veo hoy en día se implementan en Linux con VMware, por lo que gran parte de este artículo muestra, como ejemplos, cómo las soluciones integran la tecnología snapshot de VMware.

Backup de Caché

El backup online de Caché se incluye de forma predeterminada con la instalación de Caché, lo que permite la creación continua de copias de seguridad de las bases de datos de Caché. Pero hay soluciones de backup más eficientes, que se deberían considerar conforme se escalan los sistemas. El backup externo, integrado con tecnologías snapshot, es la solución recomendada para hacer copias de seguridad de sistema, incluyendo las bases de datos de Caché.

Consideraciones para los backups externos

En la documentación sobre los [Backups externos](#) están todos los detalles. Una consideración importante es:

"Para asegurar la integridad del snapshot, Caché ofrece métodos para bloquear las escrituras en la bases de datos mientras se crea el snapshot. Solo las escrituras físicas en los archivos de la base de datos se bloquean durante la creación del snapshot, lo que permite que los procesos sigan realizando actualizaciones en la memoria, sin interrupciones".

También es importante tener en cuenta que parte del proceso de snapshot en los sistemas virtualizados causa una breve pausa en la máquina virtual de la que se está haciendo la copia de seguridad, lo que a menudo se llama "stun time" (tiempo de parálisis). Esto normalmente tarda menos de un segundo, por lo que los usuarios no lo notan ni tiene un efecto sobre el funcionamiento del sistema. Sin embargo, en algunos casos la parálisis puede durar más. Si la parálisis dura más que el tiempo de inactividad permitido por el QoS para mirroring de Caché, entonces el nodo del backup creará que ha ocurrido un fallo en el primario y tomará el control. Más adelante en este artículo explicaré cómo se pueden revisar los stun times en caso de que se necesite hacer cambios en el tiempo de inactividad de mirroring en el QoS.

[Aquí puedes ver un listado con el resto de publicaciones de esta serie sobre Plataformas de datos InterSystems y su rendimiento.](#)

Para este artículo, también debes revisar la documentación de Caché: [Guía de copias de seguridad y restauración](#)

Opciones de backup

Solución de backup mínima: Backup Online de Caché

Si no se tiene otra opción, este viene incluido de forma predeterminada con la plataforma de datos InterSystems, y permite realizar copias de seguridad sin interrupción del servicio. Recuerda que el backup online de Caché solo hace una copia de seguridad de los archivos de la base de datos de Caché, en la que captura todos los bloques de las bases de datos que están asignados para datos, y escribe la salida en un archivo secuencial. El backup online de Caché admite copias de seguridad acumulativas e incrementales.

En el contexto de VMware, un backup online de Caché es una solución de copia de seguridad "in-guest" (para el sistema operativo invitado). Como otras soluciones "in-guest", las operaciones de la copia de seguridad online de Caché son esencialmente las mismas tanto si la aplicación está virtualizada como si se ejecuta directamente en un equipo. El backup online de Caché debe coordinarse con un backup del sistema, y así copiar el archivo de salida del backup online (.cbk) a una unidad de backup, junto con otros archivos del sistema que esté usando tu aplicación. Como mínimo, una copia de seguridad del sistema debe incluir el directorio de instalación, los directorios de journal y alternate journal, los archivos de aplicación y cualquier otro directorio que contenga archivos externos usados por la aplicación.

El backup online de Caché debe considerarse como una opción básica para sitios menores que desean implementar una solución económica, únicamente para crear copias de seguridad de bases de datos de Caché o copias de seguridad específicas. Es útil, por ejemplo, en la configuración de mirroring. Sin embargo, conforme las bases de datos aumentan en tamaño, y como Caché normalmente es solo una parte del ecosistema de datos de un cliente, se recomienda usar backups externos junto con tecnologías snapshot y utilidades de terceros. Esta es la práctica recomendada, que presenta ventajas como incluir el backup de archivos que no son bases de datos, menores tiempos de restauración, visión de los datos de toda la empresa y mejores herramientas de catalogación y administración.

Solución de backup recomendada: Backup Externo

Utilizando VMware como ejemplo, la virtualización en VMware añade funciones y opciones adicionales para proteger máquinas virtuales completas. Una vez que has virtualizado una solución, has encapsulado tu sistema eficazmente (incluyendo el sistema operativo, la aplicación y los datos), todo dentro de archivos .vmdk (y algunos otros). Cuando es necesario, es muy fácil administrar estos archivos y usarlos para recuperar un sistema completo. Esta misma situación es muy distinta en un sistema físico, en el que debes recuperar y configurar los componentes por separado: sistema operativo, drivers, aplicaciones de terceros, base de datos y archivos de base de datos, etc.

Snapshot de VMware

La aplicación vSphere Data Protection (VDP) de VMware y otras soluciones de terceros para realizar backups de máquinas virtuales, como Veeam o Commvault, aprovechan las funciones de los snapshots de VMware para crear copias de seguridad. A continuación, explicaré en detalle los snapshots de VMware. Para obtener más información, consulta la documentación de VMware.

Es importante recordar que los snapshots se aplican a toda la máquina virtual y que el sistema operativo y cualquier aplicación o el motor de la base de datos no saben que se están haciendo los snapshots. Recuerda también que: >

¡Por sí mismos, los snapshots de VMware no son copias de seguridad!

Los snapshots permiten a las aplicaciones de backup crear copias de seguridad, pero no son copias de seguridad en sí mismas.

VDP y otras soluciones para backups de terceros usan el proceso de snapshots de VMware, junto con la aplicación de backup, para gestionar la creación y, lo que es muy importante, la eliminación de los snapshots. El proceso y secuencia de eventos para la creación de una copia de seguridad externa con snapshots de VMware es el siguiente:

- Un software de backup solicita al host ESXi crear un snapshot de VMware.
- Los archivos .vmdk de una máquina virtual se ponen en un estado de solo lectura y se crea un archivo delta vmdk secundario para cada archivo .vmdk.
- Se usa una copia en modo escritura con todos los cambios para la máquina virtual escritos en los archivos delta. Todas las lecturas se hacen primero desde el archivo delta.
- El software de backup gestiona la copia de los archivos .vmdk principales de solo lectura en el backup de destino.
- Cuando se completa la copia de seguridad, el snapshot se confirma (los discos de la máquina virtual retoman las escrituras y los bloques actualizados en los archivos delta se escriben en el controlador).
- Ahora se elimina el snapshot de VMware.

Las soluciones de backup también usan otras funciones como Change Block Tracking (CBT) para realizar copias de seguridad incrementales o acumulativas, para mejorar la velocidad y eficiencia (especialmente importante para ahorrar espacio) y en general también agregan otras funciones importantes como la deduplicación y compresión de datos, planificación, montaje de máquinas virtuales con direcciones IP cambiadas para verificaciones de integridad, etc., restauraciones totales de máquina virtual y a nivel de archivo y administración de catálogo.

Los snapshots de VMware que no se gestionan correctamente o se dejan funcionando durante un largo tiempo pueden ocupar un espacio de almacenamiento excesivo (si cada vez más datos cambian, los archivos delta siguen creciendo) y también ralentizar las máquinas virtuales.

Debes pensar con cuidado antes de ejecutar un snapshot manual sobre una instancia de producción. ¿Por qué quieres hacer esto? ¿Qué pasará si vuelves atrás en el tiempo al momento en que se creó el snapshot? ¿Qué les sucederá a todas las transacciones de aplicación entre el momento de creación y el momento de volver atrás?

Está bien si tu software de backup crea y elimina un snapshot. El snapshot solo debería existir por un corto plazo. Y una parte clave de tu estrategia de backup será elegir un momento en que el sistema tenga baja carga, para minimizar el impacto sobre los usuarios y el rendimiento.

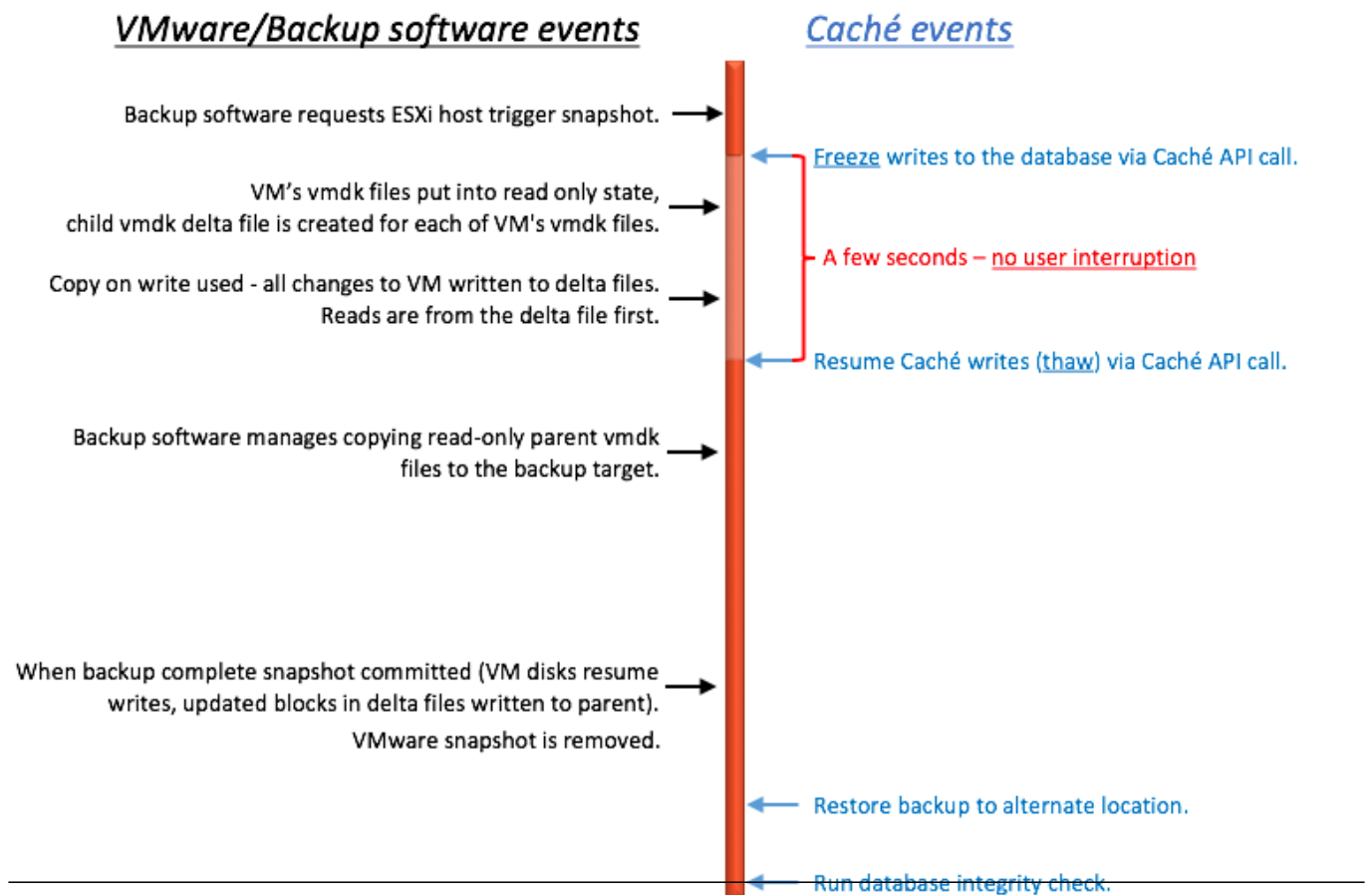
Consideraciones de la base de datos de Caché para snapshots

Antes de ejecutar el snapshot, la base de datos se debe poner en modo inactivo, de forma que todas las escrituras pendientes se confirmen y la base de datos quede en un estado consistente. Caché cuenta con métodos y una API para confirmar y luego detener (freeze) las escrituras a las bases de datos durante el breve periodo en el que se crea el snapshot. De esta forma, sólo las escrituras físicas en los archivos de la base de datos se paran durante la creación del snapshot, lo que permite que los procesos sigan realizando actualizaciones en la memoria de forma ininterrumpida. Una vez que se active el snapshot, las escrituras en la base de datos se reinician (thaw) y el backup sigue copiando datos a la unidad física. El tiempo entre el freeze y el thaw debe ser muy breve (unos pocos segundos).

Además de pausar las escrituras, el freeze de Caché también gestiona el cambio de los archivos de registro (journals) y escribe un marcador de backup en el fichero de journal. Los journals se seguirán escribiendo normalmente mientras que las escrituras a la base de datos física están detenidas. Si el sistema sufriese un fallo mientras las escrituras en la base de datos física están detenidas, los datos se recuperarían de los journals durante el arranque.

El siguiente diagrama muestra el freeze y el thaw con los pasos del snapshot de VMware para crear una copia de seguridad con una imagen consistente de la base de datos.

VMware snapshot + Caché freeze/thaw timeline (not to scale)



Fíjate en el poco tiempo entre freeze y thaw - apenas el tiempo necesario para crear el snapshot, no el tiempo para copiar el padre de solo lectura en el destino del backup.

Integración de freeze y thaw de Caché

vSphere permite invocar automáticamente un script de cualquier lado de la creación del snapshot. Este es el momento en el que se invoca el freeze y thaw de Caché. Nota: para que esta funcionalidad funcione correctamente, el host ESXi requiere que el sistema operativo invitado desactive los discos a través de VMware Tools.

Las herramientas VMware Tools deben instalarse en el sistema operativo invitado.

Los scripts deben cumplir estrictas reglas de nomenclatura y ubicación. También deben definirse los permisos de archivo. Para VMware en Linux, los nombres de los scripts son:

```
# /usr/sbin/pre-freeze-script
```

```
# /usr/sbin/post-thaw-script
```

A continuación, se muestran ejemplos de scripts de freeze y thaw que nuestro equipo usa con el backup Veeam para nuestras instancias de pruebas internas en laboratorio, pero estos scripts también deberían funcionar con otras soluciones. Estos ejemplos fueron probados y usados en vSphere 6 y Red Hat 7. >

Aunque es posible usar estos scripts como ejemplos y para ilustrar el método, ¡debes validarlos para tus

propios entornos!

Ejemplo de script pre-freeze:

```
#!/bin/sh
#
# Script invocado por VMWare inmediatamente antes de la toma del snapshot para el backup.
# Tested on Red Hat 7.2
#

LOGDIR=/var/log
SNAPLOG=$LOGDIR/snapshot.log

echo >> $SNAPLOG
echo "`date`: Pre freeze script started" >> $SNAPLOG
exit_code=0

# Only for running instances
for INST in `ccontrol qall 2>/dev/null | tail -n +3 | grep '^up' | cut -c5- | awk '{print $1}'`; do

    echo "`date`: Attempting to freeze $INST" >> $SNAPLOG

    # Detailed instances specific log
    LOGFILE=$LOGDIR/$INST-pre_post.log

    # Freeze
    csession $INST -U '%SYS' "##Class(Backup.General).ExternalFreeze(\"$LOGFILE\",,,,
,,1800)" >> $SNAPLOG $
    status=$?

    case $status in
        5) echo "`date`: $INST IS FROZEN" >> $SNAPLOG
            ;;
        3) echo "`date`: $INST FREEZE FAILED" >> $SNAPLOG
            logger -p user.err "freeze of $INST failed"
            exit_code=1
            ;;
        *) echo "`date`: ERROR: Unknown status code: $status" >> $SNAPLOG
            logger -p user.err "ERROR when freezing $INST"
            exit_code=1
            ;;
    esac
    echo "`date`: Completed freeze of $INST" >> $SNAPLOG
done

echo "`date`: Pre freeze script finished" >> $SNAPLOG
exit $exit_code
```

Ejemplo de script thaw:

```
#!/bin/sh
#
# Script called by VMWare immediately after backup snapshot has been created
# Tested on Red Hat 7.2
```

```
#

LOGDIR=/var/log
SNAPLOG=$LOGDIR/snapshot.log

echo >> $SNAPLOG
echo "`date`: Post thaw script started" >> $SNAPLOG
exit_code=0

if [ -d "$LOGDIR" ]; then
    # Only for running instances
    for INST in `ccontrol qall 2>/dev/null | tail -n +3 | grep '^up' | cut -c5- | awk
' {print $1} '`; do
        echo "`date`: Attempting to thaw $INST" >> $SNAPLOG

        # Detailed instances specific log
        LOGFILE=$LOGDIR/$INST-pre_post.log

        # Thaw
        csession $INST -U%SYS "##Class(Backup.General).ExternalThaw(\"$LOGFILE\")" >>
$SNAPLOG 2>&1
        status=$?

        case $status in
            5) echo "`date`: $INST IS THAWED" >> $SNAPLOG
                csession $INST -U%SYS "##Class(Backup.General).ExternalSetHistory(\"$L
OGFILE\")" >> $SNAPLOG$
                ;;
            3) echo "`date`: $INST THAW FAILED" >> $SNAPLOG
                logger -p user.err "thaw of $INST failed"
                exit_code=1
                ;;
            *) echo "`date`: ERROR: Unknown status code: $status" >> $SNAPLOG
                logger -p user.err "ERROR when thawing $INST"
                exit_code=1
                ;;
        esac
        echo "`date`: Completed thaw of $INST" >> $SNAPLOG
    done
fi

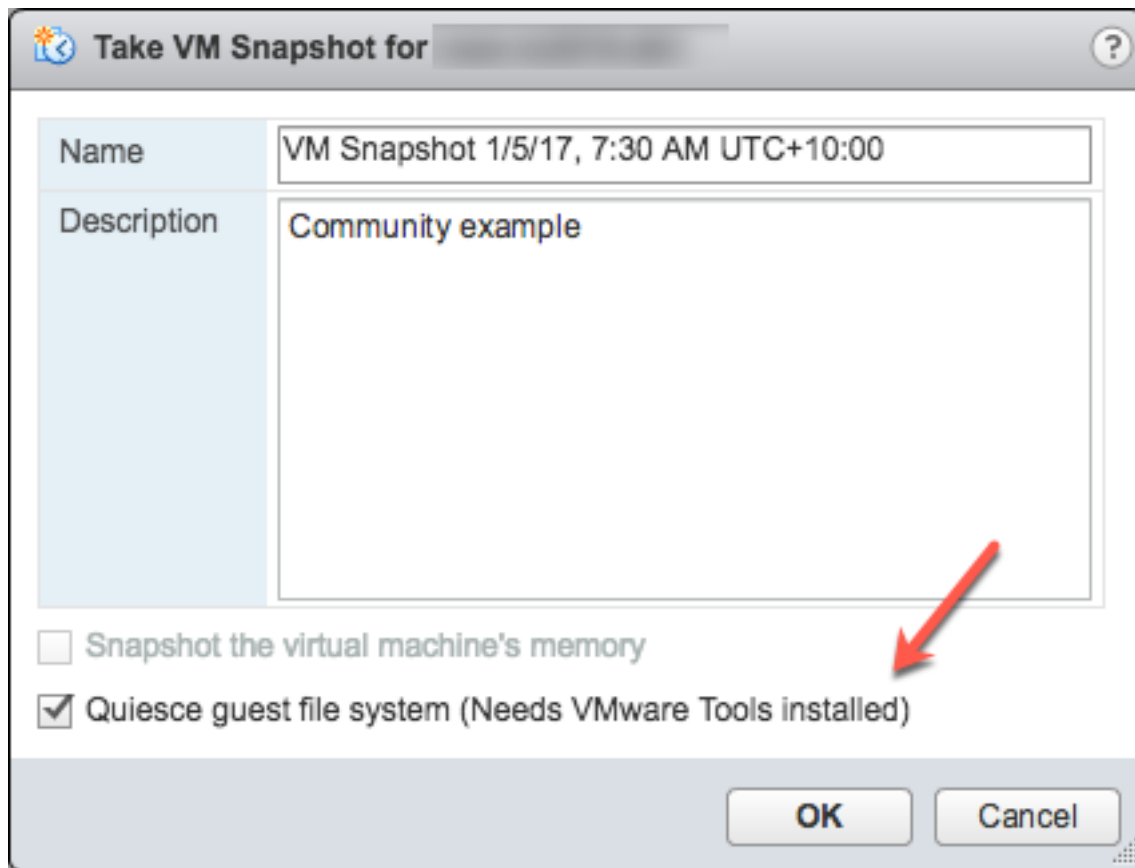
echo "`date`: Post thaw script finished" >> $SNAPLOG
exit $exit_code
```

Recuerda definir los permisos:

```
# sudo chown root.root /usr/sbin/pre-freeze-script /usr/sbin/post-thaw-script
# sudo chmod 0700 /usr/sbin/pre-freeze-script /usr/sbin/post-thaw-script
```

Prueba de freeze y thaw

Para probar que los scripts están funcionando correctamente, puedes ejecutar un snapshot manualmente sobre una máquina virtual y verificar la salida del script. La siguiente captura de pantalla muestra el cuadro de diálogo "Take VM Snapshot" y sus opciones.



Deselecciona- "Snapshot de la memoria de la máquina virtual".

Selecciona- "Desactivar sistema de archivos invitado (Necesita VMware Tools instalado)" para pausar los procesos en ejecución en el sistema operativo invitado para que los contenidos del sistema de archivos estén en un estado conocido consistente al **tomar** el snapshot.

¡Importante! ¡¡¡Después de realizar la prueba, recuerda eliminar el snapshot!!!

Si la marca de "quiesce" está activa y la máquina virtual está encendida cuando se realiza el snapshot, se usará VMware Tools para desactivar el sistema de archivos en la máquina virtual. Desactivar un sistema de archivos es el proceso de llevar los datos en disco a un estado adecuado para hacer una copia de seguridad. Este proceso podría incluir operaciones como pasar los búferes sucios desde el caché en memoria del sistema operativo hasta el disco duro.

La siguiente salida muestra los contenidos del archivo de registro \$SNAPSHOT definido en los scripts del ejemplo anterior para freeze/thaw, después de ejecutar una copia de seguridad que incluye snapshot como parte de su operación.

```
Wed Jan 4 16:30:35 EST 2017: Pre freeze script started
Wed Jan 4 16:30:35 EST 2017: Attempting to freeze H20152
Wed Jan 4 16:30:36 EST 2017: H20152 IS FROZEN
Wed Jan 4 16:30:36 EST 2017: Completed freeze of H20152
Wed Jan 4 16:30:36 EST 2017: Pre freeze script finished
Wed Jan 4 16:30:41 EST 2017: Post thaw script started
Wed Jan 4 16:30:41 EST 2017: Attempting to thaw H20152
Wed Jan 4 16:30:42 EST 2017: H20152 IS THAWED
Wed Jan 4 16:30:42 EST 2017: Completed thaw of H20152
Wed Jan 4 16:30:42 EST 2017: Post thaw script finished
```

Este ejemplo muestra que pasaron 6 segundos entre freeze y thaw (16:30:36 a 16:30:42). Las operaciones del usuario NO se interrumpen durante este periodo. Deberás recoger métricas de tus propios sistemas, pero para dar un poco de contexto, este ejemplo proviene de un sistema que ejecuta una aplicación benchmark sobre una máquina virtual sin cuellos de botella de E/S y un promedio de más de 2 millones de Glorefs/seg, 170 000 Gloupds/seg y una media de 1 100 lecturas físicas/seg y 3 000 escrituras por ciclo de daemon de escritura.

Recuerda que la memoria no es parte del snapshot, por lo que, al reiniciar, la máquina virtual se reiniciará y se recuperará. Los ficheros de la base de datos serán consistentes. No se quiere "reanudar" una copia de seguridad, sino que se quiere obtener una copia en un punto determinado en el tiempo. Luego se podrán aplicar los journals y otros pasos de recuperación necesarios para la consistencia tanto de aplicaciones como de transacciones, una vez que se han recuperado los ficheros.

Para una protección adicional de los datos, también se puede realizar un [cambio de journal](#) por sí mismo y se puede realizar una copia de seguridad de los journals o replicarlos en otra ubicación, por ejemplo, cada hora.

A continuación se muestra el resultado de \$LOGFILE en los scripts de freeze/thaw de los ejemplos anteriores, que muestran los detalles del registro para el snapshot.

```
01/04/2017 16:30:35: Backup.General.ExternalFreeze: Suspending system
```

```
Journal file switched to:
```

```
/trak/jnl/jrnpri/h20152/H20152_20170104.011
```

```
01/04/2017 16:30:35: Backup.General.ExternalFreeze: Start a journal restore for this backup with journal file: /trak/jnl/jrnpri/h20152/H20152_20170104.011
```

```
Journal marker set at
```

```
offset 197192 of /trak/jnl/jrnpri/h20152/H20152_20170104.011
```

```
01/04/2017 16:30:36: Backup.General.ExternalFreeze: System suspended
```

```
01/04/2017 16:30:41: Backup.General.ExternalThaw: Resuming system
```

```
01/04/2017 16:30:42: Backup.General.ExternalThaw: System resumed
```

STUN TIMES de máquina virtual

En el momento de creación de un snapshot de máquina virtual y después de completar la copia de seguridad y de confirmar el snapshot, la máquina virtual debe detenerse por un breve lapso. A este breve freeze a menudo se le llama "stunning" de la máquina virtual. [Aquí](#) puedes leer un buen artículo sobre los stun times. A continuación, resumo los detalles y los pongo en el contexto de la base de datos Caché.

Del artículo sobre los stun times: " Para crear un snapshot de una máquina virtual, la máquina virtual se "paraliza" para (i) serializar el estado del dispositivo al disco y (ii) cerrar el disco en ejecución actual y crear un punto de snapshot.... Al consolidar, la máquina virtual se "paraliza" para cerrar los discos y ponerlos en un estado adecuado para la consolidación. "

El stun time es normalmente de unos pocos centenares de milisegundos. Sin embargo, es posible que si hay una actividad muy elevada de escritura en disco durante la fase de confirmación, el tiempo de stun time puede ser de varios segundos.

Si la máquina virtual es un miembro Primario o de Backup que participa en el mirroring de la base de datos Caché y el stun time es mayor que el tiempo de espera del mirror de calidad de servicio (QoS), el mirror reportará un fallo de la máquina virtual donde esté el nodo primario y se producirá un failover de mirror al nodo backup o secundario.

Actualización marzo de 2018:

Mi colega Peter Greskoff me indicó que un miembro mirror del backup podría iniciar el sistema de emergencia en un tiempo tan breve como solo un poco más de la mitad del tiempo de espera de QoS durante la parálisis de una máquina virtual o en cualquier otro momento que el miembro mirror primario no esté disponible.

Para una descripción detallada de las consideraciones de QoS y escenarios de tolerancia a fallos, puedes consultar este recomendable artículo: [Guía de tiempo de espera de calidad de servicio para Mirroring](#). La versión resumida sobre los stun times de la máquina virtual y la QoS es la siguiente:

Si el mirror de la copia de seguridad no recibe mensajes del mirror primario dentro de la mitad del tiempo de espera de la QoS, enviará un mensaje para comprobar que el primario sigue funcionando. Luego, la copia de seguridad espera una respuesta de la máquina primaria durante una mitad adicional del tiempo de QoS. Si no recibe respuesta del primario, asume que no está activo y la copia de seguridad toma el control.

En un sistema con carga, se envían journals continuamente desde el mirror primario al mirror de backup, y la copia de seguridad no necesitará verificar si el primario sigue activo. Sin embargo, durante un tiempo de poca actividad (cuando es más probable que se realicen copias de seguridad), si la aplicación está inactiva es posible que no haya mensajes entre el mirror primario y la de copia de seguridad durante más de la mitad del tiempo de QoS.

Este es el ejemplo de Peter: piensa en este rango de tiempo para un sistema inactivo con un tiempo de espera de QoS de :08 segundos y un stun time de máquina virtual de :07 segundos:

- :00 el primario envía un mensaje keepalive al árbitro, el árbitro responde inmediatamente
- :01 un miembro de la copia de seguridad envía un mensaje keepalive al primario. El primario responde inmediatamente
- :02
- :03 comienza el stun de la máquina virtual
- :04 el primario intenta enviar un mensaje de keepalive al árbitro, pero no llega a destino hasta que finalice el stun
- :05 el miembro de la copia de seguridad envía un ping al primario, cuando haya vencido la mitad del QoS
- :06
- :07
- :08 el árbitro no ha recibido nada del primario durante un tiempo de espera completo de QoS, por lo que cierra la conexión
- :09 la copia de seguridad no ha obtenido respuesta del primario, y confirma con el árbitro que también perdió la conexión, por lo que asume el control
- :10 finaliza el stun de la máquina virtual, ¡¡demasiado tarde!!

Lee también la sección, "Obstáculos y preocupaciones al configurar el tiempo de espera de calidad de servicio" en la publicación indicada más arriba, para entender el equilibrio para tener QoS solo durante el tiempo necesario. Tener QoS durante demasiado tiempo, especialmente más de 30 segundos, puede causar problemas.

Fin de la actualización marzo de 2018:

Para tener más información sobre el mirroring de QoS, consulta también esta [documentación](#).

Algunas estrategias para reducir el stun time al mínimo, son crear copias de seguridad cuando la actividad de la base de datos es baja y tener un almacenamiento bien configurado.

Como se indicó más arriba al crear un snapshot, hay varias opciones que se pueden especificar- una de ellas es incluir el estado de la memoria en la snapshot. Recuerda: el estado de la memoria NO se necesita para realizar copias de seguridad de la bases de datos Caché. Si se elige la marca de memoria, se incluye en el snapshot una

copia de datos del estado interno de la máquina virtual. Lleva mucho más tiempo crear los snapshots de memoria. Los snapshots de memoria se usan para permitir la reversión a un estado de una máquina virtual en funcionamiento tal como estaba al momento del snapshot. Esto NO es necesario para realizar una copia de seguridad de archivos de una base de datos.

Al tomar un snapshot de la memoria, se paralizará todo el estado completo de la máquina virtual. El `stun time` es variable.

Como se explicó antes, para copias de seguridad se debe marcar la opción de "quiesce" para hacer snapshots manuales o que las tome el software de backup, para garantizar así una copia de seguridad consistente y utilizable.

Análisis de los `stun time` en registros de VMware

A partir de ESXi 5.0, los `stun time` por snapshot se registran en el archivo de registro de cada máquina virtual (`vmware.log`), con mensajes como estos:

```
2017-01-04T22:15:58.846Z| vcpu-0| I125: CheckpointUnstun: vm stopped for 38123 us
```

Los `stun time` están en microsegundos, por lo que en el ejemplo anterior 38123 us es 38123/1,000,000 segundos o 0.038 segundos.

Para asegurarse de que los `stun time` están dentro de los límites aceptables, o para resolver problemas si sospechas que los `stun times` prolongados generan problemas, puedes descargar y consultar los archivos `vmware.log` de la carpeta de la máquina virtual que te interesa. Una vez descargados, puedes extraer y ordenar el registro, por ejemplo usando los siguientes comandos de Linux.

Ejemplo de descarga de archivos `vmware.log`

Hay varias formas de descargar registros de soporte, incluyendo crear un paquete de soporte de VMware a través de la consola de gestión de vSphere, o desde la línea de comando del host ESXi. Consulta la documentación de VMware para obtener más detalles, pero a continuación ofrecemos un sencillo método para crear y recoger un paquete de soporte mucho más reducido, que incluye el archivo `vmware.log` para que puedas revisar los `stun times`.

Necesitarás el nombre largo del directorio donde se encuentran los archivos de la máquina virtual. Inicia sesión en el host ESXi donde se ejecuta la máquina virtual de la base de datos que utiliza ssh y usa el comando: `vim-cmd vmsvc/getallvms` para enumerar los archivos `vmx` y los nombres largos únicos asociados con ellos.

Por ejemplo, el nombre largo para la máquina virtual de la base de datos del ejemplo usado en esta publicación sale como: `26 vsan-tc2016-db1 [vsanDatastore] e2fe4e58-dbd1-5e79-e3e2-246e9613a6f0/vsan-tc2016-db1.vmx rhel764Guest vmx-11`

A continuación, ejecuta el comando para recoger y agrupar en un paquete únicamente los archivos de registro: `vm-support -a VirtualMachines:logs`.

El comando replicará la ubicación del paquete de soporte, por ejemplo: Para ver los archivos recolectados, revisa `'/vmfs/volumes/datastore1 (3)/esx-esxvsan4.iscinternal.com-2016-12-30--07.19-9235879.tgz'`.

Ahora puedes usar `sftp` para transferir el archivo hacia fuera del host para su posterior procesamiento y revisión.

En este ejemplo, después de descomprimir el paquete de soporte, ve hacia la ruta correspondiente al nombre largo de la máquina virtual de base de datos. Por ejemplo, en este caso: `/vmfs/volumes//e2fe4e58-dbd1-5e79-e3e2-246e9613a6f0`.

Ahí podrás ver varios archivos de registro numerados. El archivo de registro más reciente no tiene número, es decir vmware.log. Puede que el registro sea de unos pocos cientos de KB, pero contiene mucha información. Sin embargo, solo nos importan los stun/unstun times, que son fáciles de encontrar con grep. Por ejemplo:

```
$ grep Unstun vmware.log  
  
2017-01-04T21:30:19.662Z | vcpu-0 | I125: Checkpoint_Unstun: vm stopped for 1091706 us  
---  
  
2017-01-04T22:15:58.846Z | vcpu-0 | I125: Checkpoint_Unstun: vm stopped for 38123 us  
2017-01-04T22:15:59.573Z | vcpu-0 | I125: Checkpoint_Unstun: vm stopped for 298346 us  
2017-01-04T22:16:03.672Z | vcpu-0 | I125: Checkpoint_Unstun: vm stopped for 301099 us  
2017-01-04T22:16:06.471Z | vcpu-0 | I125: Checkpoint_Unstun: vm stopped for 341616 us  
2017-01-04T22:16:24.813Z | vcpu-0 | I125: Checkpoint_Unstun: vm stopped for 264392 us  
2017-01-04T22:16:30.921Z | vcpu-0 | I125: Checkpoint_Unstun: vm stopped for 221633 us
```

Podemos ver dos grupos de stun times en el ejemplo, uno de la creación de la snapshot, y el segundo creado 45 minutos después para cada disco cuando la snapshot se elimina/consolida (por ejemplo, después de que el software de backup haya terminado de copiar el archivo vmx de solo lectura). En el ejemplo anterior, podemos ver que la mayoría de los stun times son de menos de un segundo, si bien el tiempo de parálisis inicial es de apenas más de un segundo.

Los stun times cortos son imperceptibles para un usuario final. Sin embargo, procesos del sistema como el Mirroring de la base de datos Caché supervisan continuamente si una instancia está "viva". Si el stun time supera el tiempo de espera de QoS de mirroring, entonces el nodo podrá considerarse como no contactable y "muerto", y se activará una tolerancia de fallos.

Consejo: para revisar todos los registros o para resolver problemas, un comando útil es hacer un grep de todos los archivos vmware*.log y buscar valores atípicos o instancias en las que el stun time se aproxime al tiempo de espera de QoS. El siguiente comando canaliza la salida a awk para formatearla: `grep Unstun vmware* | awk '{ printf ("%""d", $8)} {print " ---" $0}' | sort -nr`

Resumen

Deberías supervisar tu sistema con frecuencia durante su funcionamiento normal, para entender los stun times y cómo pueden impactar sobre el tiempo de espera de QoS para aplicaciones de alta disponibilidad como mirroring. Como se indicó anteriormente, algunas estrategias para reducir los stun/unstun times al mínimo son crear copias de seguridad cuando la actividad de la base de datos y del almacenamiento es baja y tener un almacenamiento bien configurado. Para una supervisión constante, es posible procesar los registros usando VMware Log insight u otras herramientas.

En futuras publicaciones volveré a tratar las operaciones de backup y restauración para las plataformas de datos InterSystems. Pero por ahora, si tienes algún comentario o sugerencia basada en los flujos de trabajo de tus sistemas, compártelos en la sección de comentarios de abajo.

[#Administración del sistema](#) [#Arquitecturas y Soluciones de Negocio con InterSystems](#) [#Backup](#) [#Consejos y trucos](#) [#Despliegue](#) [#Mirroring](#) [#Caché](#) [#Documentación](#) [#InterSystems IRIS](#) [#InterSystems IRIS for Health](#)

URL de
fuente: <https://es.community.intersystems.com/post/plataformas-de-datos-intersystems-y-su-rendimiento-backups-de-vm-y-scripts-de-freezethaw-de>