IBM Spectrum Protect
Versión 8.1.0

Guía de determinación de problemas

IBM Spectrum Protect
Versión 8.1.0

Guía de determinación de problemas

Nota:
Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 235.

Esta edición se aplica a la versión 8, release 1, modificación 0 de IBM Spectrum Protect (número de producto 5725-W98, 5725-W99, 5725-X15) y a todos los releases y modificaciones posteriores mientras no se indique lo contrario en nuevas ediciones.

Contenido

Capítulo 3. Resolución de problemas del servidor de IBM Spectrum Protect . 57

Acerca de esta publicación

Esta publicación ayuda a determinar el origen de los problemas con los servidores y clientes en el entorno de IBM Spectrum Protect.

Antes de utilizar esta publicación, asegúrese de estar familiarizado con las áreas siguientes:

- El servidor de IBM Spectrum Protect y sistemas operativos de los clientes
- Los protocolos de comunicación instalados en sus sistemas cliente y servidor

A quién va dirigida esta guía

Esta guía se ha escrito para quienes administran o gestionan IBM Spectrum Protect. Del mismo modo, la información proporcionada en esta guía puede resultar útil para los business partner y cualquiera con la responsabilidad de proporcionar soporte técnico de IBM Spectrum Protect.

Debe estar familiarizado con IBM Spectrum Protect y los sistemas operativos que se utilizan para el entorno de IBM Spectrum Protect.

Publicaciones

La familia de productos de IBM Spectrum Protect incluye IBM Spectrum Protect Snapshot, IBM Spectrum Protect for Space Management, IBM Spectrum Protect for Databases y varios productos de gestión de almacenamiento de IBM®.

Para ver la documentación de productos IBM, consulte IBM Knowledge Center.

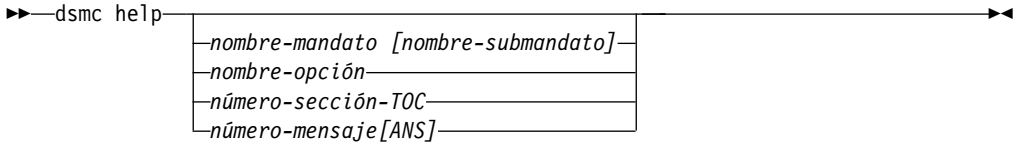
Capítulo 1. Recursos de ayuda

IBM Spectrum Protect tiene varias salidas para resolver problemas que pueda tener con el servidor o con el cliente de archivado y copia de seguridad.

Ayuda de cliente de copia de seguridad/archivado

Utilice el mandato help para obtener información sobre mandatos, opciones y mensajes. Si utiliza el mandato help en la línea de mandatos inicial, no se establecerá contacto con el servidor y no necesitará contraseña.

Sintaxis



Si introduce el mandato **HELP** sin argumentos se mostrará la tabla de contenidos completa. Tanto con el mandato inicial como cuando HELP muestra una solicitud, puede introducir los parámetros indicados a continuación.

Parámetros

command-name [subcommand-name]
Especifica un nombre de mandato y, opcionalmente, un nombre de submandato o su abreviatura. Por ejemplo: **backup image** o **b i**. En este caso, la combinación debe ser exclusiva. Las abreviaturas no únicas hacen que se muestre la primera sección del archivo de ayuda completo que coincida con dicha abreviatura. Este parámetro es opcional.

option-name
Especifica el nombre de una opción. Por ejemplo: `domain` o ***do***. Este parámetro es opcional.

TOC-section-number
Especifica una tabla del número de sección de contenido. Por ejemplo: 1.5.3. Este parámetro es opcional.

[ANS]message-number
Especifica un número de mensaje con o sin su prefijo. Por ejemplo: ans1036 o 1036. Este parámetro es opcional. El código de gravedad nunca es necesario. Si introduce ans1036E no se encontrará respuesta.

Importante: Si introduce argumentos que no coincidan con estas descripciones, puede obtener resultados inesperados (o no obtener resultados). Si introduce más de dos argumentos, su solicitud de ayuda será rechazada. Cuando el nombre de un mandato y el nombre de una opción es el mismo, por ejemplo: **incremental** (mandato) y `incremental` (opción), sólo podrá obtener ayuda para la opción introduciendo su número de sección de la tabla de contenidos.

El texto de la ayuda solicitada se mostrará en una o varias secciones, dependiendo del número de líneas de visualización disponibles en su ventana de mandatos. Una

vez que se muestre el número de líneas suficiente para llenar el espacio de visualización, o cuando se muestre el final del texto de ayuda requerido, verá una solicitud con instrucciones sobre lo que debe introducir en la misma. Para continuar mostrando texto para su selección actual, pulse **Intro** o la tecla "d" para desplazarse hacia abajo. Para desplazarse hacia arriba en la selección actual, pulse la tecla "u" y después pulse **Intro**. Utilice la tecla "q" para salir de la ayuda. Podrían presentarse otras opciones, así que lea todas las instrucciones.

Para que el texto de ayuda se muestre correctamente, la anchura de visualización utilizable debe ser de 72 caracteres. Una anchura de visualización inferior a 72 caracteres hará que las frases de 72 caracteres se corten y pasen a la siguiente línea. Esto podría provocar que el texto de ayuda mostrado comenzara en alguna parte de la sección en vez de en el principio. Las líneas que no se muestran pueden verse utilizando la función de desplazamiento del terminal para moverse hacia arriba.

Acceso a la ayuda del programa de utilidad de configuración de servicios de cliente (`dsmcutil`)

Windows

Para obtener información para el programa de utilidad deIBM Spectrum Protect Client Service Configuration, debe emitir el mandato **`DSMCUTIL HELP`**.

Cuando emite el mandato **`DSMCUTIL HELP`**, la información de ayuda se muestra dentro del programa de utilidad de ayuda deWindows.

Ayuda del agente de almacenamiento o del servidor

El servidor y el agente de almacenamiento incluyen un recurso de ayuda. El recurso de ayuda proporciona descripciones y sintaxis para mandatos del servidor y una descripción completa de los mensajes del servidor.

Acceso a la ayuda del agente de almacenamiento o del servidor para los mandatos

Emita el mandato **`HELP`** para acceder a la ayuda del agente de almacenamiento o del servidor.

Para mostrar la ayuda de línea de comandos para los comandos de servidor que tienen nombres exclusivos, puede escribir `help` *`nombre_comando`*, donde *nombre_comando* es el nombre del comando de servidor para el que desea información. Por ejemplo, para mostrar ayuda para el comando **`REGISTER NODE`**, escriba `help` *`nodo de registro.`* La sintaxis del comando y las descripciones de parámetro se muestran en la salida.

Puede escribir también `help` seguido del número de tema del comando. Los números de tema se muestran en la ayuda de línea de comandos, por ejemplo:

```
3.0 Administrative commands
  3.46 REGISTER
     3.46.1 REGISTER ADMIN (Registrar un administrador)
     3.46.2 REGISTER LICENSE (Registrar una nueva licencia)
     3.46.3 REGISTER NODE (Registrar un nodo)
```

Para mostrar ayuda sobre el comando **`REGISTER NODE`**, escriba:

```
help 3.46.3
```

Utilice números de tema para mostrar la ayuda de línea de comandos para los subcomandos. **DEFINE DEVCLASS** es un ejemplo de un comando que tiene subcomandos. Por ejemplo, puede especificar el mandato **DEFINE DEVCLASS** para las clases de dispositivo 3590 y para las clases de dispositivo 3592:

```
3.0 Administrative commands
  ...
  3.13.10 DEFINE DEVCLASS (Definir una clase de dispositivo)
      3.13.10.1 DEFINE DEVCLASS (Definir una clase de dispositivo 3590)
      3.13.10.2 DEFINE DEVCLASS (Definir una clase de dispositivo 3592)
      ...
```

Para mostrar ayuda para el mandato **DEFINE DEVCLASS** para las clases de dispositivo 3590, escriba:

```
help 3.13.10.1
```

Acceso a la ayuda para mensajes

Emita el mandato de ayuda con el fin de acceder a la ayuda para los mensajes.

Emita el comando siguiente para la ayuda sobre un mensaje del servidor: `HELP` *`número mensaje`* donde *número mensaje* es el mensaje del que desea información. Si especifica el número del mensaje sin incluir el prefijo del mensaje, por ejemplo HELP 0445, se da por supuesto el prefijo de mensaje ANR y se facilita la información de ayuda de ANR0445W. Si el número de mensaje se especifica con un prefijo, por ejemplo HELP ANR0445, se facilita la información de ayuda de ese mensaje. Emita HELP ANR0445 para ver la siguiente salida de ejemplo para ese mensaje:

```
ANR0445W Error de protocolo en la sesión núm_sesión del nodo nombre de nodo de cliente
(plataforma de cliente) - se ha sobrepasado el tamaño máximo de transacciones de grupo.
Explicación: El servidor ha detectado un error de protocolo en la sesión especificada
debido a que el cliente ha intentado agrupar más operaciones de actualización
de la base de datos que el máximo permitido en una única transacción de base de datos.
Acción del sistema: El servidor finaliza la sesión con el cliente.
Respuesta del usuario: Corrija el error de programación en el programa cliente si
se ha grabado en la instalación utilizando verbos WDSF. En cualquier otro caso,
póngase en contacto
con el representante del servicio técnico.
```

Ayuda sobre la interfaz de la línea de mandatos para el cliente

La interfaz de cliente de la línea de mandatos incluye un recurso de ayuda que ofrece descripciones y sintaxis para los mandatos y las opciones de cliente, así como una descripción completa de los mensajes de cliente.

La información de ayuda para la interfaz gráfica de usuario (GUI) y los clientes GUI de web está disponible por medio del elemento de menú **Ayuda**.

Informe de un problema relacionado con un tema de la ayuda

Cuando desee informar de un problema con el sistema de ayuda, debe reunir en primer lugar información específica.

1. Anote las selecciones que ha pulsado para obtener la ayuda. Por ejemplo, si ha pulsado en el signo de interrogación para un portal, anote el nombre del portal.
2. Visualice el código fuente de la ventana emergente de ayuda. En la mayoría de los navegadores, al realizar una pulsación con el botón derecho del ratón, se visualiza un menú con una opción **Ver código fuente**. Seleccione **Ver código**

fuente para ver el código fuente HTML para dicha ventana. Anote el título de esa ventana, que es el URL o el nombre del archivo que el sistema de ayuda intenta visualizar.

Capítulo 2. Resolución de problemas de cliente

La resolución de problemas con la aplicación cliente puede implicar la conexión con el servidor, el cambio en la configuración de políticas, la reproducción del error u otras posibles opciones.

Cómo examinar mensajes de error

Puede examinar los mensajes de error que se generan durante el funcionamiento del programa para ayudar a resolver problemas que se puedan producir.

Si se establece, la opciónCliente de IBM Spectrum Protect `QUIET` suprime la visualización de todos los mensajes en la salida de la pantalla. Sin embargo, todos los mensajes siguen registrándose en los archivos de registro. Al desactivar la opción `QUIET`, se facilitan las operaciones de resolución de problemas porque puede ver los mensajes en pantalla, cuando se producen.

Busque cualquier mensaje `ANSnnnnx` emitido a la consola. Los mensajes también se anotarán. Los mensajes de planificación se han registrado en el archivo `dsmsched.log`. Los mensajes del cliente se han registrado en el archivo `dsmerror.log`. Las descripciones de los mensajes y los códigos de retorno de la API se proporcionan en Mensajes, códigos de retorno y códigos de error. La ayuda online también está disponible para los mensajes del sistema. Para obtener ayuda online para un mensaje cuando está utilizando el cliente de la línea de mandatos,escriba **`HELP`** *ANS_nnnnx*, donde *nnnn* es el número de mensaje y *x* el tipo de mensaje.

Exploración de los mensajes de anotaciones de actividades del servidor

Utilice el mandato **`QUERY ACTLOG`** para ver el archivo de anotaciones de actividades del servidor y los mensajes emitidos para esta sesión del cliente.

Los mensajes de las anotaciones de actividades del servidor pueden facilitar más información sobre los síntomas del problema o sobre la causa real del problema que ha encontrado el cliente.

Cómo identificar el lugar y el momento en el que se puede producir el problema

Los problemas de proceso de cliente se producen a menudo cuando se realizan operaciones específicas en momentos determinados o sólo en determinadas máquinas de cliente.

Para identificar mejor el problema y cuándo aparece, determine las siguientes respuestas:

- ¿El problema se produce sólo en un cliente, en algunos clientes o en todos los clientes de un servidor determinado?
- ¿El problema se produce en todos los clientes que ejecutan en un sistema operativo en concreto?

- ¿El problema se produce en determinados archivos, en archivos de un directorio en concreto, en archivos de una unidad determinada o en todos los archivos?
- ¿El problema aparece en clientes de una red o subred específicas o en toda la red en general?
- ¿El problema se produce sólo en el cliente de la línea de mandatos, el cliente GUI o el cliente web?
- ¿IBM Spectrum Protect falla siempre al procesar el mismo archivo o directorio, o es distinto de una ejecución a otra?

Reproducción del problema

Cuando reproduzca un problema como parte de determinación de problemas, intente minimizar el impacto que tiene el proceso en IBM Spectrum Protect.

Puede ayudar al servicio de soporte de IBM Spectrum Protect minimizando la complejidad del entorno en el que desee recrear el problema. Las siguientes opciones se pueden utilizar para minimizar la complejidad del entorno:

- Utilice un archivo de opciones mínimas que sólo contenga las opciones `TCPSERVERADDRESS`, `TCPPORT` y `NODENAME`.
- Si el problema aparece en un archivo durante una copia de seguridad incremental, intente reproducir el problema con una copia de seguridad selectiva o sólo de ese archivo.
- Si el problema aparece durante un evento planificado, intente reproducir el problema ejecutando el mandato manualmente.

Recopilación de documentación para solucionar problemas con la aplicación cliente

El personal de soporte de IBM puede resolver mejor un problema si puede facilitarlos con documentación relevante. El cliente de archivado y copia de seguridad crea información en varias fuentes.

Consejo: IBM Spectrum Protect cuenta con un recurso de ayuda incorporado en la línea de mandatos del cliente. Emita el mandato **`dsmc help`** para acceder al recurso de ayuda del cliente de la línea de mandatos. El recurso de ayuda es una interfaz dirigida por menús con información que incluye referencias a los mandatos, referencias a las opciones, así como información ampliada acerca de los mensajes del cliente.

Se puede encontrar información de configuración y de problemas del cliente en uno o varios de los documentos siguientes:

- Anotaciones de errores. El archivo de registro de errores del cliente es `dsmerror.log`.
- Anotaciones de planificador. Las anotaciones de errores para el planificador cliente es `dsmsched.log`.
- Anotaciones de cliente Web. El registro de errores para el cliente web es `dsmwebcl.log`.
- Archivos de opciones. La información sobre las opciones que define paralos clientes puede facilitar la resolución de problemas. Gran parte de esta información se incluye en los siguientes archivos:
  - El archivo de opciones del cliente (`dsm.opt`). Este archivo ya existe para todos los clientes del sistema operativo.

  - El archivo de opciones de sistema del cliente (`dsm.sys`). Este archivo solo se utiliza en clientes de AIX, Linux y Mac OS X.
  - El archivo de inclusión y exclusión. Este archivo contiene los objetos que se van a incluir o excluir de las operaciones del cliente. Su ubicación se define en la opción `inclexcl`.
- Datos de rastreo. Si el programa de utilidad de trazado está activo, el archivo que contiene los datos de razado se puede proporcionar como apoyo.
- Vuelco de aplicación. Cuando el cliente de archivado y copia de seguridad del cliente deja de ejecutarse de forma inesperada, muchas plataformas generan un vuelco de la aplicación. El sistema operativo proporciona el vuelco de aplicación.
- Vuelco de memoria. Si el cliente de copia de seguridad y archivado se detiene, se puede generar un vuelco de memoria que después se puede utilizar para ayudar con el diagnóstico. El tipo de sistema determina cómo se produce el vuelco de memoria, y el sistema operativo proporciona el vuelco de memoria.

El mandato **DSMC QUERY SYSTEMINFO** está disponible y recopila la mayor parte de esta información en el archivo `dsminfo.txt`. Los siguientes elementos pueden ayudarle a determinar los problemas de IBM Spectrum Protect:

- Una lista del software que se instala en el sistema de cliente. Es posible que el cliente tenga problemas debido a interacciones con otro software en el sistema o debido a los niveles de mantenimiento de software el cliente utiliza.
- El conjunto de opciones de cliente que se define en el servidor, aplicable a este nodo cliente. Emita el mandato **QUERY CLOPTSET** para buscar los conjuntos de opciones de clientes.
- Opciones de servidor. Hay varias opciones de servidor que se utilizan para gestionar la interacción entre el cliente de archivado y copia de seguridad y el servidor. Un ejemplo de esta opción de software es `TXNGROUPMAX`.
- Información sobre este nodo tal como está definida para el servidor. Para recopilar esta información, emita el mandato **QUERY NODE** *nombre_nodo* **F=D** mediante un cliente administrativo conectado al servidor.
- Definiciones de planificación aplicables a este nodo. Las definiciones de planificación se pueden consultar desde el servidor cuando emita el mandato **QUERY SCHEDULE**.
- La información de políticas está configurada para este nodo en el servidor. La información de política se puede consultar desde el servidor cuando emita los mandatos **QUERY DOMAIN**, **QUERY POLICYSET**, **QUERY MANAGEMENTCLASS** o **QUERY COPYGROUP**.

Determine por qué razón los programas `dsmc`, `dsmadmc`, `dsm` o `dsmj` no se inician

El cliente de archivado y copia de seguridad utiliza los programas **dsmc**, **dsmadmc**, **dsm** o **dsmj** en el procedimiento de inicio. Cuando uno de estos programas no se inicia, el cliente de archivado y copia de seguridad no se iniciará.

Los programas **dsmc**, **dsmadmc**, **dsm**, o **dsmj** tienen las siguientes definiciones:

dsmc El cliente de línea de mandatos de archivado y copia de seguridad.

dsmadmc
El cliente de línea de mandatos de administración.

Windows **dsm**

AIX Linux **dsmj**

La interfaz gráfica de usuario (GUI) del cliente de archivado y copia de seguridad. La versión de tiempo de ejecución de Oracle Java™ se comprueba cuando inicia por primera vez la GUI de Java. En algunos casos, esta comprobación no se completa correctamente y el inicio de **dsm** o **dsmj** puede fallar con un mensaje "bad number".

Las detenciones de proceso y el siguiente mensaje se muestran si el programa **dsmc**, **dsmadmc**, **dsm**, o **dsmj** no se inicia:

```
ANS1398E Las funciones de inicialización no pueden abrir una de
las anotaciones o un archivo relacionado de
Registros de IBM Spectrum Protect o un archivo relacionado: dsmerror.log. errno = 13,
Los permisos de acceso de archivo no permiten la acción
especificada.
```

Recuerde: El archivo `dsmerror.log` se utiliza sólo a modo de ejemplo en el mensaje.

Las aplicaciones cliente no se ejecutarán sin poder grabar en un archivo de registro y el sistema deniega el acceso de grabación en el archivo de registro mencionado en el mensaje. Si el archivo de registro no existe, se creará con los permisos predeterminados. Se aplican las siguientes reglas:

1. Se utilizan el nombre y el directorio especificados por la opción `ERRORLOGNAME`.
2. Si no se encuentra la opción, se utiliza el nombre `dsmerror.log` del directorio especificado en la variable de entorno **DSM_LOG**, si está presente. De lo contrario, se utiliza el nombre `dsmerror.log` del directorio de trabajo actual.

Se pueden producir los siguientes problemas si se utilizan permisos predeterminados:

- El archivo de registro que se crea mediante el usuario raíz no se puede escribir mediante cualquier otro usuario
- El usuario root debe establecer los permisos adecuados o las listas de control de acceso (ACL) para permitir el uso libre de la aplicación cliente por parte de todos los usuarios que deben utilizarlo.

Si el archivo de registro se crea correctamente, una sesión sin errores deja un archivo de registro de longitud cero (vacío).

El cliente no intenta crear archivos de registro en el directorio raíz. Aparece el mensaje ANS1398E cuando el método de la primera regla, provoca que el archivo de registro se cree en el directorio raíz.

Si existe un archivo de anotaciones y se puede encontrar, IBM Spectrum Protect utiliza el método de la primera regla. También puede encontrarse en el directorio raíz, si lo elige explícitamente. Asimismo, independientemente de los permisos que otorgue, el código de IBM Spectrum Protect mantiene el archivo de anotaciones.

Cree su archivo de registro por anticipado, asegurándose de que todos los usuarios elegibles disponen de acceso de grabación. Defina la opción `ERRORLOGNAME` o la variable de entorno **DSM_DIR** para designar el archivo de registro predefinido.

Atención: Un error de archivo de anotación del sistema indica que no puede grabar en el archivo `dsmerror.log`. Es posible que determinadas aplicaciones de IBM Spectrum Protect en segundo plano no se inicien debido a errores de grabación para el archivo `dsmerror.log`. Cuando se producen estos errores, se graban determinados errores en el archivo de registro de sucesos delsistema de Windows y en el archivo de registro del sistema en otros sistemas operativos.

Windows Por ejemplo:

```
C:\Archivos de programa\Tivoli\Tsm\baclient>net start "TSM Sched"
Se está iniciando el servicio de planificación de cliente.
No se ha podido iniciar el
servicio de planificación de cliente.
Se ha producido un error específico de servidor: 12.
```

AIX Linux Mac OS X Son necesarios pasos de configuración adicionales para los usuarios que no sean root, para que puedan ejecutar las aplicaciones de IBM Spectrum Protect o IBM Spectrum Protect para las aplicaciones de protección de datos. Recibe un error ANS1398E si intenta ejecutar las aplicaciones IBM Spectrum Protect mediante un registro de errores debido a que se ha generado mediante el usuario root, que se ha quedado con los permisos predeterminados. Para la protección de datos del cliente, podrá recibir solo un error de la API de IBM Spectrum Protect. A continuación, se explica un método para configurar `dsmerror.log` de forma que puedan utilizarlo usuarios que no sean root:

1. Configure **`ERRORLOGNAME`** en `dsm.sys`. Por ejemplo, `errorLogName /var/msgs/tsm/dsmerror.log`
2. Genere **`dsmerror.log. dsmc q sess`**
3. Modifique los permisos en `dsmerror.log` para permitir la grabación por parte de todos los usuarios. `chmod 666 /var/msgs/tsm/dsmerror.log`

Resolución de problemas con conjuntos de opciones de cliente

Con los conjuntos de opciones de cliente, los administradores pueden especificar opciones adicionales que tal vez no estén incluidas en el archivo de opciones de cliente de archivo de copia de seguridad. El cliente de archivador de copia de seguridad utiliza estas opciones durante un proceso de copia de seguridad, archivado, restauración o recuperación.

Un administrador de IBM Spectrum Protect puede crear un conjunto de opciones de cliente para que las utilice un nodo de cliente en IBM Spectrum Protect. Las opciones de cliente se definen en el servidor IBM Spectrum Protect. Las opciones de cliente especificadas en el conjunto de opciones de cliente se utilizan en combinación con el archivo de opciones de cliente.

El orden en el que las opciones se procesan puede controlarse. Es posible definir varias opciones y asignarles un número de secuencia, con estas opciones procesadas desde una secuencia baja a una alta. El ejemplo siguiente muestra las opciones de **`INCLEXCL`**:

```
Opción                    Número  Alter.   Opción   Valor
                        secuen. temporal
------------      --------    --------    ---------------------------------
INCLEXCL             0          No        exclude 'sys:\backup\*'
INCLEXCL                  1        No      include  'sys:\system\*'
INCLEXCL                  2        No      include  'sys:\tmp\*'
```

Esta secuencia tiene como resultado la exclusión de todos los archivos de la vía de acceso `sys:\backup\*`, mientras que se realizan copias de seguridad de los archivos de las vías de acceso `sys:\system\*` y `sys:\tmp\*`.

Casos de ejemplo para resolver problemas con conjuntos de opciones de cliente

Utilice los conjuntos de opciones del cliente para resolver varios problemas, desde tener entornos críticos donde la restauración es una elevada prioridad, a utilizar una base de datos que no se detiene.

Consejo: La configuración del rastreo para los conjuntos de opciones de cliente se indica en el archivo de opciones de IBM Spectrum Protect para todos los clientes de archivado y copia de seguridad.

Los siguientes casos de ejemplo muestran cómo puede aprovechar el conjunto de opciones de cliente.

Caso de ejemplo 1: Tener un entorno crítico donde la restauración es una elevada prioridad.

Utilice la opción `COLLOCATEBYFILESPEC` para que todos los datos filespec se almacenen en el mínimo de cintas posible, lo cual mejorará el proceso de restauración, pues se utilizarán menos montajes de cintas. No desea que el cliente pueda alterar temporalmente esta opción. Emita el siguiente mandato del servidor:

```
Define cloptset crit_rest description="Critical Restore Option Sets"
Define clientopt crit_rest collocatebyfilespec yes force=yes
Update node dale cloptset=crit_rest
```

Caso de ejemplo 1: Utilizar estaciones de trabajo que se encuentran en una red lenta y espacio limitado para datos en el servidor.

Utilice la opción de compresión para limitar la cantidad de datos enviados y almacenados. Emita el siguiente mandato del servidor:

```
Define cloptset space_rest description="Space Restriction Option Sets"
Define clientopt space_rest compressalways no force=yes
Define clientopt space_rest compression yes force=yes
Update node mark cloptset=space_rest
```

Caso de ejemplo 1: Utilizar una base de datos que no se detiene.

Existe un problema con la base de datos puesto que los archivos están abiertos y el servidor no puede realizar una copia de seguridad de los mismos. Excluya todos los archivos y subdirectorios a partir de copias de seguridad de IBM Spectrum Protect y agregue los archivos y subdirectorios al conjunto de opciones de cliente "`space_rest`" existentes. Emita el mandato **`EXCLUDE DIR`** y especifique la vía de acceso del directorio que se va a excluir. Emita el siguiente mandato del servidor:

```
Define clientopt space_rest inclexcl "exclude.dir c:\lnotes\data"
```

Caso de ejemplo 1: Finalizar copias de seguridad utilizando una red rápida y desear realizar el mejor uso posible de los recursos de cliente.

Configure la opción `RESOURCEUTILIZATION` en la cantidad máxima. Emita el siguiente mandato del servidor:

```
Define cloptset unix_srv description="UNIX Server Option Sets"
Define clientopt unix_srv resourceutilization 10 force=yes
```

Resolución de problemas de caducidad

Si recibe un error de autenticación, es posible que sea resultado de la caducidad de una contraseña. La caducidad de la contraseña no se aplica a las contraseñas de nodo o de administrador que se autentican con un servidor de directorio LDAP.

Procedimiento

Siga estos pasos para cambiar el periodo de la contraseña expirada:

1. Para cambiar el periodo de la contraseña expirada para un nodo particular, emita el mandato de servidor **UPDATE NODE** con la opción **PASSEXP**=*n*, donde *n* es el número de días. Un valor de 0 desactiva la caducidad de la contraseña.

   Si un cliente de Windows no se puede conectar al servidor después de haber cambiado de nombre, verifique el nombre de nodo se cambió en el archivo de opciones del cliente y en el registro de Windows. Cuando el planificador del cliente se ejecuta como un proceso en primer plano y utiliza el mandato **DSMC SCHED**, IBM Spectrum Protect utiliza el nombre del nodo en el archivo de opciones de cliente para contactar con el servidor. Sin embargo, cuando el planificador se ejecuta como un servicio de Windows, IBM Spectrum Protect utiliza el nombre de nodo del registro de Windows.
2. Para el cliente de Windows, emita el mandato**DSMCUTIL UPDATE SCHEDULE** para conseguir los siguientes resultados:
   - Con el parámetro *node*, indique cómo cambiar el nombre de nodo que se utiliza con el servicio planificador de IBM Spectrum Protect en Windows
   - Con el parámetro *validate:yes*, póngase en contacto con el servidor IBM Spectrum Protect para autenticar y almacenar la contraseña actualizada.

Resolución de problemas de contraseña autenticada en LDAP

La mayoría de los problemas derivados de la autenticación de contraseñas pueden atribuirse a la conexión entre el servidor de IBM Spectrum Protect y el servidor de directorio LDAP.

Esta documentación se refiere al método de autenticación LDAP que se utiliza en servidores de versiones anteriores a la V7.1.7 y que utilizan los usuarios de IBM Security Directory Server. Para obtener más información sobre este método, consulte Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1)

Antes de poder utilizar la contraseña autenticada LDAP, debe configurar el servidor de directorio LDAP para comunicarse con el servidor deIBM Spectrum Protect. Asegúrese de que la lista de control de acceso del servidor de directorio LDAP ofrece la autoridad completa al usuario (LDAPUSER) a través de un nombre de base distinguida (Base DN).

Verificación de la configuración de autenticación de la contraseña

Si ha configurado el servidor para autenticar las contraseñas con un servidor de directorio LDAP y tiene errores, revise los pasos de configuración. Debe asegurarse de que el servidorIBM Spectrum Protect y el servidor de directorio de LDAP están configurados correctamente.

Procedimiento

1. Abra el archivo de opciones `dsmserv.opt` y busque la opción **LDAPURL**, que contiene el servidor y el nombre distinguido base (DB base). Puede añadir más valores a la opción **LDAPURL**, con cada valor de URL de hasta 1024 caracteres. El número de puerto es opcional. El número de puerto predeterminado es 389. Cada configuración de URL debe contener los siguientes valores:
   - Un nombre de servidor de directorio LDAP
   - La DN de base del espacio de nombres o el sufijo del servidor de directorio LDAP se mantiene. El formato del DN debe cumplir con el servidor de directorio que elija.

   La opción **LDAPURL** debe cumplir las siguientes especificaciones:
   - Si especifica varias URLs, siga estas indicaciones:
     - Todas las URL deben estar en una línea separada
     - Cada URL debe apuntar a un directorio externo diferente y todos los directorio externos deben contener los mismos datos
   - Cada URL debe comenzar con el siguiente valor: `ldap://`

   Por ejemplo:

   ```
   LDAPURL ldap://zapp.storage.dallas.gov/ou=tsmdata,dc=storage,dc=dallas,dc=com
   ```

   La URL que especifica no puede ser una URL segura, esto quiere decir que no puede comenzar con `ldaps://`.
2. Visualice los ajustes de **LDAPUSER** o **LDAPPASSWORD** emitiendo el mandato **QUERY STATUS**. Defina al usuario **LDAPUSER** que puede añadir o eliminar entradas y cambie o restaure las contraseñas. Si el **LDAPUSER** no está definido, emita el mandato **SET LDAPUSER** para definir el administrador del servidor de directorio LDAP.

   Importante: Si el valor para el parámetro **LDAPUSER** incluye caracteres especiales, delimite el valor con comillas dobles. Por ejemplo:

   ```
   set ldapuser "cn=bill cook,cn=users,dc=storage,dc=dallas,dc=gov"
   ```
3. Visualice los ajustes de **LDAPUSER** o **LDAPPASSWORD** emitiendo el mandato **QUERY STATUS**. Si no hay definida una contraseña, designe una para **LDAPUSER** emitiendo el mandato **SET LDAPPASSWORD**.

   A continuación se listan los caracteres que puede utilizar para una contraseña:

   ```
   a b c d e f g h i j k l m n o p q r s t u v w x y z
   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
   0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
   | { } [ ] : ; < > , ? / ~
   ```

   Requisito: Si utiliza caracteres especiales cuando emite el mandato **SET LDAPPASSWORD**, póngalos entre comillas. Por ejemplo:

   ```
   set ldappassword "Pa$$=w0rd"
   ```

El servidor de IBM Spectrum Protect no acepta el LDAPPASSWORD

Si recibe un aviso que indica que LDAPPASSWORD no es válido, es posible que el problema no sea de la contraseña.

Si emite un mandato **SET LDAPPASSWORD** y recibe los mensajes de error ANR3114E o ANR3116E, es posible que IBM Spectrum Protect no esté configurado correctamente. Examine los mensajes del servidor que se han producido alrededor de la hora en la que se emitieron ANR3114E o ANR3116E para determinar la causa de los errores. Un problema común que podría ver es que se ha configurado un valor incorrecto para el mandato **SET LDAPUSER**. El usuario debe introducirse en un formato de nombre distinguido (DN). Por ejemplo:

```
ou=armonk,cn=tsmdata,uid=9A73819745
```

Si el valor no cumple con el DN, el **LDAPUSER** no se define y no puede configurar el LDAPPASSWORD. Un DN normalmente consiste en una lista de valores separados por coma de los atributos de nombresy los pares de valores. La siguiente lista muestra los atributos de nombres que se usan con más frecuencia:

- El nombre común (cn)
- El ID de usuario (uid)
- Unidad organizativa (ou)
- El componente de dominio (dc)
- Organización (o)
- País (c)

Por ejemplo:

```
cn=Jack Spratt,ou=marketing,dc=tucson,dc=storage,dc=com
uid=abbynormal,ou=sales,dc=tucson,dc=storage,dc=com
uid=cbukowski,ou=manufacturing,o=storage,c=us
```

Resolución de problemas con el servidor de directorios LDAP

Si tiene problemas con la autenticación de contraseña, verifique si ha completado todos los pasos de configuración correctamente. ¿Ha definido el nombre distinguido base (DN base) en el servidor de directorios LDAP? ¿Ha establecido la opción **LDAPURL**?

Después de instalar el servidor de Tivoli Storage Manager V6.3.3 o posterior, o el servidor de IBM Spectrum Protect V7.1.3 o posterior, tiene que configurar el servidor de directorios LDAP para comunicarse con el servidor.

Si tiene problemas de conexión, efectúe los pasos siguientes con un programa de utilidad LDAP, por ejemplo `ldpsearc` o `ldp.exe`:

1. Pruebe la búsqueda de DNS hacia adelante y hacia atrás del sistema servidor LDAP en el sistema servidor.
2. Pruebe la conexión de red entre el sistema operativo de servidor y el sistema operativo de servidor de directorios LDAP.
3. Conéctese al servidor de directorios LDAP con el nombre de host y el puerto especificados en la opción **LDAPURL**.
4. Establezca una conexión TLS (Transport Layer Security - Seguridad de la capa de transporte) emitiendo la opción **StartTLS**.
5. Utilice la autenticación de enlace simple para autenticarse con los parámetros que ha definidos para **LDAPUSER** y **LDAPPASSWORD**.

6. Busque en el servidor de directorios de LDAP el DN base que ha especificado en la opción **LDAPURL**.

Un administrador de servidor LDAP puede utilizar el programa de utilidad **ldapsearch**, de la manera siguiente, para solucionar problemas de autenticación de directorio LDAP:

Utilizando OpenLDAP (especifique el archivo de certificado utilizando la opción TLS_CACERT en el archivo ldap.conf)
Sin SSL/TLS

```
ldapsearch -H <hostname>
-D <LDAPUSER> -W -s base -b
<BaseDN from LDAPURL> -v -x objectclass="*"
```

Con SSL/TLS

```
ldapsearch -H <hostname>
 -D <LDAPUSER> -W -s base -b
<BaseDN from LDAPURL> -v -x -ZZ objectclass="*"
```

Utilizando el cliente LDAP (instalado con AIX o descargado de ibm.com)
Sin SSL/TLS

```
ldapsearch -h <hostname>
-D <LDAPUSER>  -w ? -s base -b
<BaseDN from LDAPURL> -v objectclass="*"
```

Con SSL/TLS

```
ldapsearch -h <hostname>
-D <LDAPUSER> -w ? -s base -b
<BaseDN from LDAPURL> -v -Y -x -K "cert.kdb" objectclass="*"
```

Para los mandatos anteriores, se aplican los parámetros siguientes:

- *nombrehost* = URL de la opción **LDAPURL**, por ejemplo
  `ldap://ldap.ibm.com:389/`
- *LDAPUSER* = parámetros del mandato **SET LDAPUSER**, por ejemplo
  `cn=tsmserver,cn=users,dc=ibm,dc=com`
- *DN base de LDAPURL* = DN base de la opción **LDAPURL**, por ejemplo
  `"OU=tsm,DC=ibm,DC=com"`

Resolución de problemas con nodos y administradores bloqueados

Las contraseñas que se autentican en el servidor de directorios LDAP pueden quedar bloqueadas si se sobrepasa el límite de contraseñas incorrectas o por acciones del administrador.

Procedimiento

Si no se puede desbloquear una contraseña bloqueada, realice los pasos siguientes:

1. Devuelva la contraseña al servidor de emitiendo el siguiente mandato de ejemplo:

   ```
   update node node_x new_pw authentication=local
   ```

2. Limpie el servidor de directorios LDAP emitiendo el siguiente mandato de ejemplo:

   ```
   audit ldapdirectory fix=yes wait=no
   ```

   Este mandato elimina nodos o ID de administrador que están almacenados en el servidor de directorios LDAP que no autentican contraseñas en un servidor de directorios LDAP.

3. Cierre sesión en el nodo.

4. Emita el siguiente mandato:
   `update node node_x newest_pw authentication=ldap`
5. Inicie sesión en el nodo con la contraseña nueva.

Auditoría del servidor de directorios LDAP para limpiar el servidor

Si se mantiene el servidor de directorios de LDAP sincronizado con el servidor de , resulta más sencillo saber con qué se está trabajando. El servidor de directorios LDAP puede tener cientos de entradas que ya no se utilizan. También es posible que en el servidor de directorios LDAP falten determinadas entradas de administración o de nodo que se supone que están en el servidor de directorios LDAP.

Una auditoría puede informarle sobre el registro de entradas de nodo o ID de administrador que han autenticado las contraseñas en el servidor de directorios LDAP. Puede auditar el servidor de directorios LDAP para borrar las contraseña, los administradores y los nodos no utilizados. El espacio de nombres controlado de IBM Spectrum Protect en el servidor de directorios LDAP puede quedar fuera de sincronización con lo que está almacenando el servidor IBM Spectrum Protect.

Si el administrador del servidor de directorios LDAP ha cambiado manualmente entradas en el directorio externo, esas entradas no estarían en sincronización. El servidor IBM Spectrum Protect también puede quedar sin sincronización con el servidor LDAP cuando se utiliza el mandato **SYNCLDAPDELETE=NO** predeterminado durante un mandato **REMOVE**, **RENAME** o **UPDATE** . El mandato **AUDIT LDAPDIRECTORY** suprime todas las entradas del servidor de directorios LDAP que no se correlacionan con la base de datos de IBM Spectrum Protect. El mandato también emite avisos para ayudarle a arreglar los elementos.

Se emiten avisos si las contraseñas que se autentican en el servidor de directorios LDAP se almacenan en la base de datos de IBM Spectrum Protect pero no en el espacio de nombres LDAP. Desde los avisos, puede utilizar el mandato **UPDATE NODE** o **UPDATE ADMIN** para corregir el problema.

Ejemplo: Auditoría del servidor de directorios LDAP

Si el espacio de nombres de IBM Spectrum Protect en el servidor de directorios LDAP no está en sincronización con la base de datos de IBM Spectrum Protect, emite el mandato siguiente:

```
AUDIT LDAPDIRECTORY FIX=YES
```

El mandato produce una lista de todos los nodos y administradores que se suprimen del servidor de directorios LDAP. También se produce una lista de todos los nodos y administradores que faltan en el servidor de directorios LDAP. Si desea ver qué elementos están fuera de sincronización, utilice el valor predeterminado **FIX=NO** para informar de las discrepancias entre los servidores.

Nota: No utilice el valor **FIX=YES** si varios servidores IBM Spectrum Protect comparten el espacio de nombres de directorio LDAP.

Mensajes de error para contraseñas LDAP autenticadas

Al autenticar contraseñas con un servidor de directorio LDAP, se pueden producir errores habituales durante la conexión entre el servidor y el servidor de directorio LDAP.

Estos mensajes de error son resultado de comunicarse con un servidor de directorio LDAP:

ANR3114E

El mensaje ANR3114E se emite cuando se produce un error inesperado durante una operación LDAP. El mensaje le proporciona más información para asistirle en la resolución del error. Por ejemplo,

```
Error ANR3114E de LDAP
LDAP error code (error description) ocurrido durante operation.
```

Código de error LDAP

El número de error que se devuelve bien mediante la interfaz de cliente LDAPo el servidor de directorio LDAP.

descripción del error

Una descripción del *LDAP error code* (código de error LDAP), indicando la causa del error.

operación

La operación del cliente LDAP que se está ejecutando cuando se ha producido el error.

En el siguiente ejemplo, el código de error 53 se devuelve a la interfaz del cliente LDAP o el servidor de directorio LDAP. La operación que estaba en progreso en el momento en el que se marcó el error. En este ejemplo, ldap_search_s.

```
ANR3114E
Error LDAP 53 (DSA is unwilling to perform) se ha producido ldap_search_s.
```

ANR3115E

El mensaje ANR3115E se emite cuando hay un error con el servidor de directorio LDAP. Por ejemplo,

```
ANR3115E The LDAP directory server returned the following error message
(LDAP server message) with the LDAP error.
```

Mensaje de error LDAP

El servidor de directorio LDAP devuelve este mensaje y da más información sobre el error que acaba de ocurrir.

ANR3116E

El mensaje de error ANR3116E se emite cuando el componente de Global Security ToolKit (GSKit) se encuentra con un error durante una operación LDAP. GSKit proporciona Secure Sockets Layer/Transport Layer Security (SSL/TLS) para las operaciones de LDAP. Este mensaje de error está relacionado con los certificados SSL/TLS, la criptografía o las operaciones de red. Por ejemplo:

```
Error ANR3116E LDAP SSL/TLS GSKIT error code
(error description) se ha producido durante operation.
```

Código de error GSKit

El número de error que devuelve el componente GSKit.

descripción del error

Una descripción del texto asociado con el *error code* (código de error) que indica la causa del error.

operación
La operación del cliente LDAP que se está ejecutando cuando se ha producido el error.

Si no puede determinar la causa de los errores, siga estos pasos:

1. Examine los mensajes del servidor que se emitieron a la misma hora que se produjo el error para determinar la causa y el impacto del error. Emita el mandato **QUERY ACTLOG** para ver el archivo de registro de la actividad y buscar los mensajes de error.
2. Compruebe si hay problemas relacionados con la red.
3. Compruebe el estado del servidor de directorio LDAP.
4. Para el mensaje de error ANR3116E, busque los problemas con los certificados que el servidor de directorio LDAP utiliza o la base de datos clave del servidor deIBM Spectrum Protect (`cert.kdb`).
5. Examine los archivos de registro del servidor de directorio LDAP.
6. Utilice los programas de utilidad LDAP como “ldapsearch” o “ldp” para aislar el problema .

La tabla siguiente contiene errores que se puede encontrar si la configuración no es correcta:

Tabla 1. Errores que se pueden producir cuando autentica contraseñas con un servidor de directorio LDAP

Mensajes de error	Solución
ANR3114E Error LDAP 118 (La biblioteca SSL no se puede cargar) ANR3116E Error LDAP SSL/TLS 118 (Error SSL desconocido) ANR3103E Se ha producido un error al inicializar los servicios de directorio LDAP	Es posible que la vía de acceso a biblioteca no esté configurada correctamente. Asegúrese de que está utilizando la versión correcta de GSKit.
ANR3114E Error LDAP 116 (No se ha podido establecer conexión con el servidor SSL) ANR3116E Error LDAP SSL/TLS 406 (Error de E/S) ANR3103E Se ha producido un error al inicializar los servicios de directorio LDAP ANR2732E No se puede comunicar con el servidor de directorio LDAP	El nivel de GSKit puede ser incorrecto en Directory Server. Actualice GSKit al nivel correcto. Consulte la nota técnica 1469388. En Active Directory, inhabilite las actualizaciones de certificados raíz automáticas con Windows Update si no hay disponible una conexión a Internet.
ANR3114E Error LDAP 52 (DSA no está disponible) ANR3103E Se ha producido un error al inicializar los servicios de directorio LDAP ANR2732E No se puede comunicar con el servidor de directorio LDAP	El servidor de Active Directory no tiene un certificado disponible para TLS/SSL. Cree un certificado firmado que pueda utilizar Microsoft Active Directory.

Tabla 1. Errores que se pueden producir cuando autentica contraseñas con un servidor de directorio LDAP (continuación)

Mensajes de error	Solución
ANR3114E Error LDAP 116 (No se ha podido establecer conexión con el servidor SSL) ANR3116E Error LDAP SSL/TLS 414 (Certificado erróneo) ANR3103E Se ha producido un error al inicializar los servicios de directorio LDAP ANR2732E No se puede comunicar con el servidor de directorio LDAP	El certificado de servidor de directorio LDAP no es de confianza. Añada el certificado de entidad emisora de certificados raíz (CA) al archivo de base de datos de claves IBM Spectrum Protect (`cert.kdb`) y verifique que los certificados no han caducado.
ANR3094E El nombre distinguido (DN) que se especifica en la opción **LDAPURL** no existe en el servidor de directorio LDAP ANR3103E Se ha producido un error al inicializar los servicios de directorio LDAP	Si existe el ND, puede que **LDAPUSER** no tenga derechos completos de control de acceso al ND Base DN que se especifica en la opción**LDAPURL** .
ANR3114E Error LDAP 50 (Acceso insuficiente) ANR1885E Inicialización de servicio de directorios LDAP: Se ha denegado el permiso cuando se ha accedido a la entrada de directorio LDAP como LDAPUSER ANR3103E Se ha producido un error al inicializar los servicios de directorio LDAP ANR1885E SET LDAPPASSWORD: Se ha rechazado el permiso cuando se ha accedido a la entrada **LDAPUSER**	**LDAPUSER** no tiene derechos de control de acceso completos al DN base especificado en la opción **LDAPURL** .
ANR3114E Error LDAP 116 (No se ha podido establecer conexión con el servidor SSL) ANR3116E Error SSL/TLS de LDAP 420 (Socket cerrado)	Para Directory Server, SSL_TIMEOUT_MILLISEC no se ha establecido en un valor suficientemente alto. Consulte la nota técnica 1233758.
ANR3114E Error de LDAP 4 (Se ha superado el límite de tamaño)	Aumente el límite de tamaño de búsqueda de servidor LDAP para acomodar el número total de administradores y nodos autenticados en LDAP.
El error ANR3114E LDAP 91 (Error de conexión) se ha producido durante ldap_sasl_bind. El fallo ANR3103E se ha producido al inicializar los servicios del directorio LDAP.	El servidor LDAP no está activo o está desconectado.

Resolución de problemas de planificación del cliente

El administrador para IBM Spectrum Protect puede planificar las tareas para ejecutarse automáticamente.

Si tiene problemas con el planificador cliente, los siguientes pasos de diagnóstico pueden ayudarle a determinar la causa del problema:

- El planificador cliente no reconoce los cambios ni las adiciones en las opciones de cliente hasta que se inicia el siguiente planificador. Las supresiones realizadas al conjunto de opciones del cliente no tienen efecto hasta que reinicia el planificador.
- Las adiciones, las supresiones y los cambios realizados a las planificaciones gestionadas por la aceptación del cliente se reconocen en el siguiente inicio planificado.
- Utilice el programa de utilidad de diagnóstico **SHOW PENDING** para mostrar planificaciones, nodos y el siguiente tiempo de ejecución planificado.
- Desde el archivo de opciones del cliente, consulte la stanza `dsm.sys` para el nodo y los valores de las opciones `MANAGEDSERVICES`, `PRESCHEDCMD` y `POSTSCHEDCMD` para obtener más información una vez que un nodo omita un evento planificado.

Determinación del estado de un evento planificado

El servidor mantiene un registro de todos los eventos planificados. Los registros son útiles para gestionar planificaciones de IBM Spectrum Protect en numerosos sistemas del cliente.

Acerca de esta tarea

Siga estos pasos para ver los registros de eventos en un servidor:

Procedimiento

1. Emita el mandato **QUERY EVENT**.
2. Emita la siguiente consulta para ver todos los resultados de eventos para el día anterior:

   ```
   query event * * begindate=today-1 begintime=00:00:00
   enddate=today-1 endtime=23:59:59
   ```

3. Emita la siguiente consulta para limitar los resultados de ésta a los casos de excepción.

   ```
   query event * * begindate=today-1 begintime=00:00:00
   enddate=today-1 endtime=23:59:59 exceptionsonly=yes
   ```

Qué hacer a continuación

Los resultados de la consulta incluyen un campo de estado que ofrece un resumen del resultado de un evento concreto. Al utilizar la opción `format=detailed` también puede ver el resultado de un evento que es el código de retorno general que devuelve el cliente. Consulte el mandato **QUERY EVENT** para conocer detalles sobre los sucesos planificados y completados.

Comprobación de errores en las anotaciones de actividades del servidor

Si falta un evento planificado pero otros eventos planificados para ese nodo muestran un resultado de `Completado`, compruebe los errores de las anotaciones de actividades del servidor y las anotaciones de planificación del cliente.

Al consultar las anotaciones de actividades del servidor, céntrese sólo en los resultados de consulta del intervalo de tiempo sobre el evento planificado. Comience la solicitud de anotaciones de eventos en un momento algo anterior a la ventana de inicio de ese evento planificado. Por ejemplo, investigue el siguiente evento sospechoso:

```
Inicio planificado   Inicio real Nombre planif. Nombre nodo Estado
------------------- ------------ ------------- ------------ -------
08/21/2003           08:27:33    CADA HORA      NODEA       Inexistente
```

Posteriormente, puede emitir una de las siguientes consultas:

```
query actlog begind=08/21/2003 begint=08:25:00
query actlog begind=08/21/2003 begint=08:25:00 originator=client node=nodea
```

El cliente guarda un registro detallado de todas las actividades planificadas. Consulte las anotaciones de planificación locales del cliente si las solicitudes de las anotaciones de actividades del servidor no pueden explicar el error en el evento planificado.

Debe tener acceso al sistema del cliente para inspeccionar el archivo de anotaciones de planificación. El registro de planificación normalmente se guarda en el archivo`dsmsched.log` en el mismo directorio que el archivo `dsmerror.log`. La ubicación del archivo de registro se puede especificar utilizando opciones de cliente, de modo que es posible que necesite consultar el archivo de opciones para ver si se ha utilizado la opción `SCHEDLOGNAME` para reubicar el archivo de registro. En Windows, el registro de planificación se puede reubicar con un ajuste que es parte de la definición de servicio planificada. Puede emitir el mandato **DSMCUTIL QUERY** para comprobar si configuró esta opción. Al ubicar las anotaciones de planificación, busque en el archivo el intervalo de tiempo que corresponda con la fecha y la hora de inicio de ese evento en concreto. La siguiente lista muestra los parámetros de búsqueda comunes:

- Si está investigando un evento inexistente, consulte los detalles del evento anterior, incluida la hora en la que se completó el evento anterior.
- Si está investigando un error de evento, busque los mensajes de error que expliquen el error (como que se hayan excedido los límites de sesión de servidor).
- Cuando una explicación siga sin estar clara, el último lugar para buscar es el archivo de registro de errores del cliente (normalmente llamado `dsmerror.log`).

Inicio y detención del servicio del cliente

El inicio y detención del servicio del cliente puede en ocasiones ayudar a resolver problemas de planificación de clientes.

Consejo: Si gestiona muchos clientes que ejecutan procesos de planificador, puede que desee tener la capacidad de poder iniciar y detener el servicio del cliente desde un sistema remoto. El cliente de Windows proporciona una herramienta para ayudar en la gestión remota del servicio de planificador. Para otros sistemas, se requieren herramientas estándar de sistema operativo.

Windows Para gestionar de forma remota el servicio del planificador cliente utilizando el mandato **DSMCUTIL** con la opción `/computer:`, debe tener derechos de administrador en el dominio del sistema destino. Para determinar si el servicio de planificador se ejecuta en un sistema remoto, compruebe el campo **Current Status** en una consulta similar a la siguiente:

```
dsmcutil query /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com
```

Emita las consultas siguientes para reiniciar el servicio de planificador al que le faltan planificaciones:

```
dsmcutil stop /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com
dsmcutil start /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com
```

Por lo tanto, si utiliza el CAD (client acceptor daemon) para gestionar el planificador, puede que tenga que reiniciar el servicio CAD o detener el servicio de planificador y reiniciar el servicio de CAD con las siguientes consultas:

```
dsmcutil query /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com
dsmcutil query /name:"TSM Client Acceptor" /computer:ntserv1.ibm.com
dsmcutil stop /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com
dsmcutil stop /name:"TSM Client Acceptor" /computer:ntserv1.ibm.com
dsmcutil start /name:"TSM Client Acceptor" /computer:ntserv1.ibm.com
```

AIX Linux Si utiliza el método tradicional para gestionar el planificador, puede escribir un script de shell para buscar y detener la ejecución de planificadores o procesos de aceptación de clientes de IBM Spectrum Protect y reiniciar, a continuación, los procesos. El siguiente script de shell de ejemplo muestra cómo reprocesar el proceso de planificador de IBM Spectrum Protect:

```
#!/bin/ksh
# Utilice el script siguiente para terminar la instancia en ejecución
# del planificador de TSM y reinicie el planificador en modo nohup.
#
# Este script no funcionará adecuadamente si hay más de un proceso de
# planificador en ejecución.
# En caso necesario, se pueden personalizar las siguientes variables
# para permitir la utilización
de un archivo de opciones alternativo.
# export DSM_DIR=
# export DSM_CONFIG=
# export PATH=$PATH:$DSM_DIR
# Extraiga el PID para el planificador TSM que se está ejecutando
PID=$(ps -ef | grep "dsmc sched" | grep -v "grep" | awk {'print $2'});
print "Proceso original del planificador de TSM con PID=$PID"
# Terminación del planificador mediante el mandato kill
kill -9 $PID
# Reinicie el planificador con nohup, redirigiendo toda la salida a NULL
# La salida seguirá registrada en dsmsched.log
nohup dsmc sched 2>&1 > /dev/null &
# Extraiga el PID para el planificador TSM que se está ejecutando
PID=$(ps -ef | grep "dsmc sched" | grep -v "grep" | awk {'print $2'});
print "Nuevo proceso del planificador de TSM con PID=$PID"
```

AIX Linux Mac OS X Si desea utilizar el método CAD gestionado para gestionar el planificador del cliente, defina la opción `managedservices` a **`schedule`** o **`schedule webclient`** en el archivo `dsm.sys`. Para Mac OS X, si no especifica la opción `managedservices`, CAD gestiona tanto el planificador como el cliente web, de forma predeterminada.

AIX Agregue la siguiente entrada en el archivo de inicio del sistema (`/etc/inittab` en la mayoría de las plataformas):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # TSM Client
Acceptor Daemon
```

Linux El programa de instalación del cliente de archivado y copia de seguridad crea un script de inicio de sesiónpara el CAD (**`dsmcad`**) en el directorio `/etc/init.d`. Puede iniciar, detener, reiniciar y consultar el CAD utilizando el mandato**`service`** estándar en Linux. Por ejemplo:

```
# service dsmcad start
# service dsmcad stop
# service dsmcad restart
# service dsmcad statis
```

Para activar el CAD para que se inicie automáticamente después de reiniciar el sistema, añada el servicio como sigue, en el indicador de shell:

```
# chkconfig --add dsmcad
```

Mac OS X Puede iniciaro detener el CAD con el programa de utilidad **`launchd`**. Para iniciar el CAD, emita el siguiente mandato en la ventana Terminal:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Para detener el CAD, emita el siguiente mandato en la ventana Terminal:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

También puede controlar el CAD con la aplicación **TSM Tools for Administrators**.

Resolución de problemas al incluir o excluir archivos de cliente durante el proceso de copia de seguridad

La opción de proceso include/exclude afecta a qué archivos se envían al servidor para una operación de copia de seguridad o de archivado. Son posibles varios motivos si se indica de manera implícita o explícita que un archivo se incluya o se excluya durante el proceso de copia de seguridad y no se ha procesado correctamente.

Identificación de archivos incluidos o excluidos por el conjunto de opciones del cliente del servidor.

El administrador de IBM Spectrum Protect puede incluir o excluir archivos en beneficio del cliente. Las sentencias de inclusión o exclusión que provienen del servidor modificarán las sentencias de inclusión y exclusión entradas en el archivo de opciones del cliente local.

Póngase en contacto con el administrador del servidor IBM Spectrum Protect para corregir el problema.

Puede emitir el mandato **DSMC QUERY INCLEXCL** de cliente de archivado y copia de seguridad para identificar los archivos que incluye o excluye el conjunto de opciones de cliente del servidor. La salida de este mandato muestra "Sistema operativo" como archivo de origen para los archivos que se excluyeron automáticamente del proceso de copia de seguridad. En nuestro ejemplo, los usuarios indicaron que deseaban que todos los archivos que acabasen con la extensión ".o" se incluyeran en el archivo de opciones local, pero el servidor envió al cliente una opción para excluir todos los archivos que acabaran con la extensión ".o". Prevalece la opción proporcionada por el servidor.

```
tsm> q inclexcl
*** ARCHIVO DE INCLUSIÓN/EXCLUSIÓN ***
Modo Función   Patrón (de arriba abajo)       Archivo de origen
---- --------- ------------------------------ -----------------
Excl All       /.../*.o                         Servidor
Incl All       /.../*.o                         dsm.sys
```

Las opciones que se transfieren al cliente desde el servidor se suministran en grupos, lo que significa que si las opciones `INCLUDE` y `EXCLUDE` se admiten en el servidor y todas las opciones de `INCLUDE` se envían en un grupo y todas las opciones de `EXCLUDE` en otro. No se puede entremezclar esas opciones para obtener los resultados deseados de incluir algunos archivos de directorios excluidos. Utilizar la opción `INCLEXCL` permite mezclar y ordenar las opciones `INCLUDE` y `EXCLUDE`.

Exclusión automática de archivos del proceso de copia de seguridad

La aplicación de copia de seguridad no realiza una copia de seguridad de archivos concretos porque no son necesarios para una copia de seguridad, o IBM Spectrum Protect utiliza los archivos para el proceso interno.

Si los archivos concretos deben incluirse en el proceso de copia de seguridad, IBM Spectrum Protect puede incluirlos si coloca las sentencias *INCLUDE* en el conjunto de opciones de cliente establecido en el servidor.

Importante: Puesto que algunos archivos se identificaron explícitamente como archivos de los que no se realiza copia de seguridad, no los incluya en el conjunto de opciones de cliente de servidor.

Emita el mandato **DSMC QUERY INCLEXCL** del cliente de archivado y copia de seguridad para identificar los archivos de los que no se realizó copia de seguridad. La salida del mandato **DSMC QUERY INCLEXCL** muestra "Sistema operativo" como archivo de origen para los archivos que se excluyeron automáticamente del proceso de copia de seguridad.

Windows Por ejemplo, se muestra la siguiente salida cuando emite el mandato **DSMC QUERY INCLEXCL**:

```
tsm> q inclexcl
*** ARCHIVO DE INCLUSIÓN/EXCLUSIÓN ***
Modo Función   Patrón (de arriba abajo)       Archivo de origen
---- --------- ------------------------------ -----------------
Excl All       C:\WINDOWS\Registration\*.clb  Sistema operativo
Excl All       C:\WINDOWS\netlogon.chg        Sistema operativo
```

Consulte Tabla 2 en la página 24 para conocer los archivos que se han excluido automáticamente.

Tabla 2. Archivos excluidos automáticamente durante el proceso de copia de seguridad

Plataforma	Archivos excluidos

Windows	• Archivos que se enumeran en la clave de registro `HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`
	• El directorio intermedio del cliente `C:\ADSM.SYS`
	• Metarchivos IIS (Internet Information Server) (estos archivos se procesan en el objeto del sistema o en la copia de seguridad de estado del sistema)
	• Archivos de registro (esos archivos se procesan en el objeto del sistema o en la copia de seguridad de estado del sistema)
	• Archivos de rastreo de cliente
	• Archivos de sistema
	Los archivos de sistema Windows se excluyen silenciosamente del proceso de copia de seguridad de la unidad del sistema y no se pueden incluir.
	Para procesar estos archivos de sistema Windows, debe emitir un mandato **DSMC BACKUP SYSTEMSTATE**.
	Los archivos de los sistemas Windows se excluyen del proceso de copia de seguridad de la unidad del sistema porque normalmente se envían durante las copias de seguridad del estado del sistema o del objeto del sistema. Los archivos del sistema son archivos de arranque, de catálogo, contadores de rendimiento y los archivos protegidos por Protección de archivos del sistema (sfp) de Windows. Estos archivos no se procesan durante la copia de seguridad de la unidad del sistema. Sin embargo, los archivos se excluyen del proceso de la unidad del sistema internamente en lugar de depender de sentencias de exclusión explícitas, debido al elevado número de sentencias de exclusión que se necesitarían para representar todos esos archivos. El rendimiento de las copias de seguridad puede verse afectado negativamente.
	Puede emitir el mandato **DSMC QUERY SYSTEMINFO** del cliente de archivado y copia de seguridad para identificar los archivos del sistema Windows. La salida de este comando se graba en el archivo `dsminfo.txt`.
	`(contenido parcial del archivo dsmfino.txt)`
	`==========`
	`SFP`
	`c:\windows\system32\ahui.exe (protegido)`
	`c:\windows\system32\apphelp.dll (protegido)`
	`c:\windows\apppatch\apphelp.sdb (protegido)`
	`c:\windows\system32\asycfilt.dll (protegido)`

AIX Linux	Archivo de rastreo de cliente
Mac OS X	• Archivos volátiles, temporales y de dispositivo que utiliza el sistema operativo • Archivos de rastreo de cliente

Exclusión de archivos con la sentencia EXCLUDE.DIR

La sentencia EXCLUDE.DIR excluye todos los directorios y archivos del directorio padre.

Si desea incluir todos los archivos que coinciden en un patrón de archivo, independientemente de su ubicación dentro de una estructura de directorio, no utilice las sentencias EXCLUDE.DIR.

Por ejemplo, considere este conjunto de sentencias de exclusión/inclusión:

AIX Linux Mac OS X

```
exclude.dir /usr
include     /.../*.o
```

Windows

```
exclude.dir C:\Users
include C:\...\*.o
```

La sentencia INCLUDE de este ejemplo indica que todos los archivos con una extensión .o se deben incluir, pero la sentencia EXCLUDE.DIR precedente excluirá todos los archivos del directorio /usr o C:\Users aunque tengan una extensión .o. Este hecho se cumplirá, independientemente del orden de las sentencias.

Si desea hacer una copia de seguridad de todos los archivos que terminen en .o, utilice la sintaxis siguiente: AIX Linux Mac OS X

```
exclude     /usr/.../*
include     /.../*.o
```

Windows

```
exclude C:\Users\...\*
include C:\...\*.o
```

Cuando utilice caracteres comodín, utilice * si desea incluir o excluir todos los archivos en vez del patrón *.*.*.*. El patrón *.*.*.* significa que se deben incluir o excluir todos los archivos que contienen al menos un punto (.), mientras que * significa que se deben incluir o excluir todos los archivos. Si utiliza *.*, todos los archivos que contengan caracteres sin punto (como C:\MYDIR\MYFILE en Windows) no se filtran.

Si desea ejecutar una copia de seguridad selectiva o una copia de seguridad parcial incremental de un único archivo desde el cliente de línea de mandatos, no se verá afectada por la opción EXCLUDE.DIR.

Si utiliza un cliente de línea de mandatos para iniciar una copia de seguridad selectiva o una copia de seguridad parcial incremental de un único archivo, se procesará el archivo, incluso si hay una sentencia que EXCLUDE.DIR que excluya uno de los directorios padre en la vía de acceso del archivo.

Por ejemplo, piense en la siguiente sentencia de inclusión-exclusión que se utiliza en acciones de línea de mandatos posteriores: AIX Linux Mac OS X

```
exclude.dir /home/spike
```

Windows

```
exclude.dir C:\Users\spike
```

La siguiente copia de seguridad selectiva siempre da como resultado el archivo en proceso: AIX Linux Mac OS X

```
dsmc selective /home/spike/my.file
```

Windows

```
dsmc selective C:\Users\spike\my.file
```

Si emite una copia de seguridad selectiva utilizando un comodín, no se procesa ningún archivo porque el directorio está excluido: AIX Linux Mac OS X

```
dsmc selective "/home/spike/my.*"
```

Windows

```
dsmc selective "C:\Users\spike\my.*"
```

Importante: Una copia de seguridad incremental posterior del sistema de archivos `/home` dejará inactivo el archivo `/home/spike/my.file`. Del mismo modo, en Windows una copia de seguridad incremental posterior del directorio `C:\Users` hace que el archivo `C:\Users\spike\my.file` se quede inactivo.

No termine las sentencias `EXCLUDE.DIR` con un delimitador de directorio.

Los siguientes ejemplos muestran las sentencias incorrectas `EXCLUDE.DIR`, debido a un delimitador de directorio al final de la vía de acceso de directorio: AIX Linux

```
exclude.dir /usr/
```

Mac OS X

```
exclude.dir /Users/
```

Windows

```
exclude.dir c:\directory\
```

Los ejemplos siguientes muestran la codificación correcta de `EXCLUDE.DIR`: AIX Linux

```
exclude.dir /usr
```

Mac OS X

```
exclude.dir /Users
```

Windows

```
exclude.dir c:\directory
```

Determinar si las sentencias de compresión, cifrado y copia de seguridad de subarchivos incluyen o excluyen

Las sentencias de inclusión y exclusión de compresión (INCLUDE.COMPRESS), cifrado (INCLUDE.ENCRYPT) y copia de seguridad de subarchivos (INCLUDE.SUBFILE) no implican la inclusión del archivo en el proceso de copia de seguridad.

Puede utilizar las sentencias INCLUDE y EXCLUDE en combinación con las sentencias COMPRESS, ENCRYPT y SUBFILE para obtener los resultados deseados.

Consulte el ejemplo siguiente: AIX Linux Mac OS X

```
exclude          /usr/file.o
include.compress /usr/*.o
```

Windows

```
exclude c:\Users\file.o
include.compress c:\Users\*.o
```

Esta sentencia indica que el archivo `/usr/file.o` está excluido del proceso de copia de seguridad. La sentencia INCLUDE.COMPRESS indica que "si un archivo es candidato a un procesamiento de copia de seguridad y coincide con el patrón `/usr/*.o` se comprime el archivo." No debe interpretarse la sentenciaINCLUDE.COMPRESS como "realizar la copias de seguridad de todos los archivos que coinciden con`/usr/*.o` y comprimirlos." Si desea realizar una copia de seguridad del archivo `/usr/file.o` de este ejemplo, debe eliminar la sentencia de exclusión.

Uso de delimitadores para incluir o excluir archivos

Cuando los limitadores de volumen o de directorio no son correctos, pueden provocar que las sentencias `INCLUDE` y `EXCLUDE` no funcionen adecuadamente.

Las sentencias `INCLUDE` o `EXCLUDE` específicas de plataforma contienen sintaxis para "todo" y "todos los archivos en un directorio específico".

Si desea utilizar una sentencia `INCLUDE` para "todos los archivos en un directorio específico", compruebe que todas las barras inclinadas y los delimitadores de volúmenes sean correctos. Si desea incluir todos los archivos situados en un directorio llamado "home", consulte los ejemplos siguientes:

Windows **Uso de la contrabarra inclinada "\" y el delimitador de volumen ":"**

```
*incluir todo en el directorio c:\home
include c:\home\...\*
*incluir todo
include *:\...\*
```

AIX Linux Mac OS X **Uso de la barra inclinada "/"**

```
*incluir todo en el directorio /home
include /home/.../*
*incluir todo
include /.../*
```

Resolución de errores debidos a la lista de inclusión y exclusión codificada incorrectamente

Debido a la complejidad o al número de sentencias INCLUDE o EXCLUDE, puede experimentar la inclusión o exclusión no deseada de un archivo.

Configure el cliente con el indicador de rastreo **INCLEXCL** para que le ayude a determinar el motivo por el que se ha incluido o excluido un archivo.

Por ejemplo, cuando crea que el archivo `c:\home\file.txt` debe estar incluido en el proceso de copia de seguridad. El rastreo muestra que existe una sentencia EXCLUDE que excluye el archivo:

```
polbind.cpp (1026): Archivo 'C:\home\file.txt' excluido de forma explícita
por el patrón
'Excl All c:\home\*.txt'
```

El uso del mandato **DSMC QUERY INCLEXCL** del cliente de archivado y copia de seguridad muestra que esta sentencia se encuentra en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect:

```
tsm> q inclexcl
*** ARCHIVO DE INCLUSIÓN/EXCLUSIÓN ***
Modo Función   Patrón (de arriba abajo)       Archivo de origen
---- --------- ------------------------------ -----------------
Excl All       c:\home\*.txt                  Servidor
```

Resolución de problemas de Snapshot Difference

AIX Linux Windows

Puede realizar copias de seguridad incrementales de volúmenes de archivador N-Series y NetApp si utiliza la interfaz de programación de aplicaciones (API) de NetApp Snapshot Difference.

Requisitos previos

Para utilizar la característica de Snapshot Difference, antes debe configurar un ID de usuario y una contraseña de NetApp en el cliente. El ID de usuario y la contraseña son necesarios para que IBM Spectrum Protect se conecte con el Archivador. Configure un ID de usuario/contraseña con autoridad raíz enAIX y Linux o uno con autoridad administrativa en Windows. Configure el nivel de nivel de autorización de forma que sea igual al nivel de autorización utilizado al correlacionar o montar el volumen del archivador. Asegúrese de utilizar el nombre de host completo o el formato con puntos de dirección IP para el nombre del archivador. Emita el mandato de cliente de archivado y copia de seguridad **SET PASSWORD** para guardar este ID de usuario/contraseña.

Recuerde: El mandato **DSMC SET PASSWORD** se amplía para escribir contraseñas “filer”.

La característica Snapshot Difference compara dos instantáneas (base y diferencial) y devuelve una lista de los archivos modificados, eliminador o añadidos entre las dos. IBM Spectrum Protect realiza una copia de seguridad de esta lista de archivos en vez de explorar el sistema de archivos en busca de cambios.

La característica Snapshot Difference admite las siguientes características (sólo aplicables al nivel de volumen):

- Archivadores NetApp/N-Series que ejecutan Data ONTAP release 7.3 o posterior
- Windows Volúmenes Common internet files system-attached (CIFS)
- Volúmenes de archivador tradicionales y FlexVol
- GUI Java y cliente web
- AIX Linux Volúmenes adjuntos Network file system (NFS)

La característica Snapshot Difference no admite las siguientes características:

- Volúmenes adjuntos SAN NetApp/N-Series
- QTrees o subdirectorios
- Los volúmenes VFiler con un archivador que se ejecuta en ONTAP V8.1.0 o versiones anteriores no son compatibles. Los volúmenes Vfiler con un archivador que se está ejecutando en ONTAP V8.1.1 o posterior son compatibles.

Windows

Verificación del tipo de volumen del Archivador

IBM Spectrum Protect espera que el tipo de seguridad CIFS (Common Internet Files System-attached) sea New Technology File System (NTFS). Utilice NetApp FilerView y asegúrese de que el tipo de seguridad CIFS es “ntfs.”

Restricciones de Snapshot Difference

La falta de soporte Unicode de NetApp evita que IBM Spectrum Protect procese archivos que utilicen caracteres que no se encuentre dentro del rango ASCII de 7 bits. IBM Spectrum Protect puede realizar copias de seguridad solo de nombres que contengan caracteres ASCII. Al probar caracteres Unicode se han señalado dos comportamientos de Snapshot Difference:

1. El mandato incremental de Snapshot Difference finaliza con el código de retorno 13001. Este código de retorno se produce con los rangos "especiales" y "sustitutos" de Unicode para los volúmenes del archivador de Snapshot Difference que se crean con el distintivo UTF8. Este error de Snapshot Difference se produce frecuentemente sin el distintivo UTF8. IBM Spectrum Protect finaliza con el mensaje de error ANS5283E “La operación no se ha realizado correctamente.” No se ha realizado copia de seguridad de ningún archivo.
2. La interfaz de programación de aplicaciones (API) de Snapshot Difference no falla, pero devuelve caracteres que no forman parte del nombre real. IBM Spectrum Protect inspecciona la serie para ver si algún carácter se encuentra fuera del rango ASCII de 7 bits. De ser así, IBM Spectrum Protect salta el archivo y registra el error en el archivo `dsmerror.log`.

A continuación se indican algunas situaciones en las que podría no realizarse copia de seguridad de los archivos y directorios y en las que no se informaría de ningún error:

- Para excluir un archivo debe añadir una regla de exclusión en el archivo de inclusión/exclusión. IBM Spectrum Protect realiza una copia de seguridad de la instantánea actual teniendo en cuenta la regla de exclusión. No debe cambiar el archivo, pero debe eliminar la regla que ha excluido el archivo. Los mandatos de copia de seguridad incremental asistidos por instantánea con la opción `snapdiff` no detectan este cambio de inclusión/exclusión porque sólo detectan cambios de archivos entre dos instantáneas. Los archivos en sí deben modificarse para que la API de Snapshot Difference detecte el cambio y para que IBM Spectrum Protect realice una copia de seguridad del archivo.

- Añadió una sentencia de inclusión al archivo de opciones. Esto incluye que la sentencia solo tiene lugar si el archivo ha sufrido cambios realizados por la API Difference. No se puede realizar una copia de seguridad de los archivos porque IBM Spectrum Protect no inspecciona cada archivo en el volumen durante la operación de copia de seguridad.
- Suprime de forma explícita un archivo del inventario de IBM Spectrum Protect emitiendo el mandato **DSMC DELETE BACKUP**. La API de Snapshot Difference no detecta si un archivo se ha suprimido manualmente de IBM Spectrum Protect. Por ello, el archivo permanece sin protección en el almacenamiento. El archivo permanece sin protección hasta que éste se modifica en el volumen y el cambio es detectado por la API de Snapshot Difference. Después del cambio, la API de Snapshot Difference API señala IBM Spectrum Protect para que realice la copia de seguridad del archivo de nuevo.
- Los cambios de política como el cambio de Mode=modified a mode=absolute no se detectan. El espacio de archivos completo se suprime del inventario. Las políticas no detectadas hacen que IBM Spectrum Protect cree una instantánea que será utilizada como origen (base) y se realizará una copia de seguridad incremental completa.

La ejecución de una copia de seguridad incremental sin la opción `snapdiff` resuelve estas limitaciones. IBM Spectrum Protect no controla lo que constituye un objeto cambiado. Ahora los cambios de objeto los controla la API de Snapshot Difference. Así, la ejecución de una copia de seguridad incremental completo sin la opción `SNAPDIFF` garantiza la detección de todos los cambios en archivos.

Puede utilizar los siguientes distintivos de rastreo para el proceso de Snapshot Difference:

- `enter`
- `exit`
- `general`
- `snapshot`
- `hci`
- `hci_detail`
- `diskmap`
- `diskmap_detail`
- `hdw`
- `hdw_detail`
- `bacache`
- `snapdiffdb`

AIX Linux

Configure un ID de usuario y una contraseña para root en el archivador myFiler.ibm.com.

```
dsmc set password -type=filer myFiler.ibm.com root
```

```
Por favor, introduzca la contraseña para el ID de usuario "root@myFiler.ibm.com": ********
Vuelva a introducir la contraseña para su verificación:********
ANS0302I Operación correcta.
```

AIX Linux

Configure un ID de usuario y una contraseña para root en el archivador myFiler.ibm.com.

```
dsmc set password -type=filer myFiler.ibm.com root secret
```

Resolución de problemas del directorio de instantáneas para volúmenes de sistemas de archivos NetApp o N-Series

Cuando se realiza la copia de seguridad de un volumen de network file system (NFS) montado o un Common Internet File System (CIFS) correlacionado, también se realiza una copia de seguridad de todas las instantáneas del directorio `snapshot`. Esta copia de seguridad incluye instantáneas no deseadas que pueden ocupar espacio valioso. Los volúmenes de NFS montado o de CIFS correlacionado pueden ser NetApp o N-Series.

Para evitar una copia de seguridad de instantáneas no deseadas, utilice el método de copia de seguridad NDMP (Network Data Management Protocol). También puede realizar una copia de seguridad de sus datos con la opción de cliente `SNAPSHOTROOT` o ejecutar una copia de seguridad incremental con el mandato **`INCREMENTAL`** y la opción `SNAPDIFF`. De forma alternativa, puede excluir el directorio `snapshot` de cualquier copia de seguridad.

Importante: Linux Si ejecuta una copia de seguridad de NetApp SnapDiff completa y después utiliza el método NFS4 para montar el volumen de NetApp en el servidor, se produce otra copia de seguridad de NFS. Para evitar una copia de seguridad completa, utilice el distintivo de prueba**SNAPDIFFINCR** para forzar el procesado incremental en las entradas que ya se han procesado. Por ejemplo, `-test=snapdiffincr`.

Resolución de problemas de inicio de sesión al utilizar el sistema de archivos cifrados en sistemas operativos AIX

AIX

Durante el proceso de inicio de sesión, el almacén de claves del sistema de archivos cifrados (EFS) se abre automáticamente cuando la contraseña del almacén de claves coincide con la contraseña de inicio de sesión del usuario.

Cuando la contraseña de inicio de sesión en AIX es diferente a la contraseña del almacén de claves EFS, debe abrir dicho almacén de claves de forma manual antes de iniciar el cliente. Abra el almacén de claves emitiendo el mandato siguiente:

```
efskeymgr -o <cmd>
```

Inicie el cliente de una de las maneras siguientes:

- Inicie el cliente de la línea de mandatos emitiendo el mandato `efskeymgr -o ./dsmc`.
- Inicie el cliente GUI de Java emitiendo el mandato `efskeymgr -o ./dsmj`.

Si está utilizando la interfaz gráfica de usuario (GUI) web del cliente, debe sincronizar las contraseñas. Para sincronizar la contraseña de usuario con la contraseña de almacén de claves EFS, emita el mandato siguiente:

```
efskeymgr -n
```

Resolución de errores de copia de seguridad de imágenes

AIX Linux

Los errores de copia de seguridad de imagen se pueden producir con imágenes Linux, imágenes de Linux Snapshot, o durante la copia de seguridad de imágenes y el archivado y copia de seguridad basado en instantáneas de AIX JFS2.

Resolución de errores de copia de seguridad de imagen de Linux

Linux

Puede resolver errores de copia de seguridad de imagen de Linux siguiendo pasos específicos, en función del tipo de error que se produzca.

Acerca de esta tarea

Se ha generado el siguiente error durante la copia de seguridad de imagen:

```
paris:#dsmc b image /dev/system/lv01
Se ha llamado a la función de copia de seguridad de imagen.
ANS1228E No se ha podido enviar el objeto '/dev/system/lv01'
ANS1584E Error al cargar la biblioteca del sistema 'libdevmapper.so'
necesaria para operaciones con imágenes en volúmenes LVM2.
ANS1813E El proceso de copia de seguridad de imagen de '/dev/system/lv01'
ha finalizado con errores.
Número total de objetos inspeccionados: 1
Número total de objetos de copia de seguridad: 0
Número total de objetos actualizados: 0
Número total de objetos revinculados: 0
Número total de objetos suprimidos: 0
Número total de objetos caducados: 0
Número total de objetos con errores: 1
Número total de bytes transferidos: 0 B
Tiempo de transferencia de datos: 0.00 seg
Velocidad de transferencia de datos de red: 0.00 KB/seg
Velocidad de transferencia de datos compuesta: 0.00 KB/seg
Objetos comprimidos en: 0%
Tiempo transcurrido en el proceso: 00:00:29
paris# cat dsmerror.log
11/15/2006 13:07:53 ANS1228E No se ha podido enviar el objeto
'/dev/system/lv01'
11/15/2006 13:07:56 ANS1584E Error al cargar la biblioteca del
sistema 'libdevmapper.so' necesaria para
operaciones con imágenes en volúmenes LVM2.
11/15/2006 13:07:56 ANS1813E El proceso de copia de seguridad de imagen
de '/dev/system/lv01' ha finalizado
con errores.
```

En el caso de este error, asegúrese de que el sistema tiene instalada la versión correcta del correlacionador de dispositivos de bibliotecas. Siga estos pasos para determinar la versión instalada:

Procedimiento

1. Emita el mandato **# DMSETUP VERSION**. La salida es similar a esta:

   ```
   Versión de biblioteca:   1.00.09-ioctl (2004-03-31)
   Versión de controlador:    4.4.0
   ```

   o

   Emita el siguiente mandato para determinar la versión mediante rpm:

   ```
   # rpm -q -a |grep device-mapper
   ```

La salida es similar a esta:

```
device-mapper-1.00.09-17.5
```

La versión de la biblioteca debe ser la 1.01 o superior.

2. Verifique la instalación tras la actualización.

```
# rpm -Uvh device-mapper-1.01.01-1.6.i586.rpm
Preparing... ########################################### [100%]
1:device-mapper ########################################### [100%]
# rpm -q -a |grep device-mapper
device-mapper-1.01.01-1.6
```

También puede comprobar el directorio /lib para ver si las versiones instaladas son correctas. Un sistema con los niveles correctos mostrará la siguiente información:

```
#  ls -l /lib/libdev*
lrwxrwxrwx 1 root root 20 Jul 5 11:42 /lib/libdevmapper.so
->libdevmapper.so.1.01
-rwxr-xr-x  1 root root 24490 May 23  2005 /lib/libdevmapper.so.1.00
-rwxr-xr-x  1 root root 28216 May 23  2005 /lib/libdevmapper.so.1.01
```

Resolución de anomalías de copia de seguridad cuando se utiliza la copia de seguridad de instantánea de Linux

Linux

Para resolver una copia de seguridad de imágenes de instantánea de Linux anómala, compruebe que el sistema está configurado para crear una instantánea.

Antes de empezar

Intente crear una instantánea desde un indicador de la shell emitiendo el mandato siguiente:

```
/sbin/lvcreate -L 16384K -n <snapname eg. tsmsnap>-s
<volume devname eg /dev/system/lv01>
```

Si recibe el error `Snapshot: Required device-mapper target(s) not detected in your kernel`, significa que el módulo de kernel **:dm_snapshot** no está cargado. Este mandato podría fallar también por otros motivos, que pueden provocar un comportamiento de IBM Spectrum Protect similar.

Acerca de esta tarea

El siguiente ejemplo muestra la salida generada cuando falla una copia de seguridad de imagen con el mensaje de error ANS1258E, “La operación de instantánea no se ha realizado.”

```
dsmerror.log :
05/31/2006 15:14:36 ANS1259E La operación de instantánea no se ha realizado correctamente.
Texto de diagnóstico: tsmStartSnapshot.
05/31/2006 15:14:38 ANS1259E La operación de instantánea no se ha realizado correctamente.
Texto de diagnóstico: tsmTerminateSnapshot.
05/31/2006 15:14:38 ANS1228E No se ha podido enviar el objeto '/fs1'
05/31/2006 15:14:38 ANS1258E La operación de instantánea de imagen ha fallado.
```

Procedimiento

Complete los siguientes pasos para cargar los módulos:

1. Verifique que el módulo no está cargado. Consulte el siguiente mandato de ejemplo:

```
# lsmod |grep dm_
dm_mod                112104  6
```

2. Cargue el módulo. Consulte el siguiente mandato de ejemplo:

```
# modprobe dm_snapshot
```

3. Verifique que el paso anterior se ha realizado correctamente. Consulte el siguiente mandato de ejemplo:

```
# lsmod |grep dm_
dm_snapshot            44024  0
dm_mod                112104  6 dm_snapshot
#
```

4. Cree una instantánea desde el indicador de shell. Consulte el siguiente mandato de ejemplo:

```
# /sbin/lvcreate -L 16384K -n tsmsnap -s /dev/system/lv01
Logical volume "tsmsnap" created
```

5. Elimine la instantánea que se creó en el paso anterior. Consulte el siguiente mandato de ejemplo:

```
# lvremove /dev/system/tsmsnap
¿Está seguro de que desea eliminar el volumen lógico "tsmsnap" activo? [y/n]: y
El volumen lógico "tsmsnap" se ha eliminado correctamente
#
```

Resultados

Si ha seguido todos los pasos, ahora podrá ejecutar copias de seguridad de imágenes de instantáneas.

Restricción: Si el mandato **lvcreate** falla con el error "`Insufficient free extents (0) in volume group...`", indicará que no hay suficiente espacio en el grupo de volúmenes para un volumen de instantánea.

Resolución de errores durante la copia de seguridad de imagen y copia de seguridad/archivado basado en instantáneas de AIX JFS2

AIX

Durante la finalización de IBM Spectrum Protect, el cliente elimina la instantánea del sistema de archivos de diario mejorado de AIX (JFS2) que se creó durante el proceso de copia de seguridad. Sin embargo, existen situaciones donde AIX no consiga llevar a cabo la petición de eliminación de la diapositiva realizada por IBM Spectrum Protect.

Antes de empezar

Las siguientes situaciones ilustran los casos en que la solicitud de eliminación de una instantánea puede fallar:

- Se pulsan las teclas `Control-C` durante el proceso de copia de seguridad de instantánea de IBM Spectrum Protect. La solicitud de desmontaje de instantánea de JFS2 puede fallar con el error "Dispositivo ocupado", porque el proceso de IBM Spectrum Protect se encuentra en mitad del acceso a la instantánea.
- Dos peticiones de copia de seguridad de instantánea de IBM Spectrum Protect se han iniciado simultáneamente para el mismo sistema de archivos. Por ejemplo, si la solicitud de copia de seguridad `dsmc backup image /fs1` se ha enviado desde

una consola, y al mismo tiempo se emite una solicitud de copia de seguridad `dsmc backup image /fs1` desde otra consola. Si el proceso de la primera consola crea la primera instantánea para `/fs1` y el segundo proceso de la segunda consola crea la segunda instantánea para `/fs1`, y si el segundo proceso finaliza primero e intenta eliminar la instantánea, AIX no consigue llevar a cabo la solicitud.

- Dos peticiones de copia de seguridad de instantánea de IBM Spectrum Protect se han iniciado simultáneamente para dos puntos de montaje virtuales cuyo sistema de archivos de origen es el mismo. Por ejemplo, emitir `dsmc incr /fs1/level1/dir1` desde una consola y `dsmc incr /fs1/level2/level3/dir3` desde una segunda consola, simultáneamente.

Acerca de esta tarea

AIX espera que las peticiones de eliminación de instantáneas se emitan en un cierto orden con la eliminación de la instantánea más antigua solicitada primero, y la eliminación de la siguiente instantánea más antigua solicitada a continuación, etc. Si IBM Spectrum Protect no puede aceptar la secuencia a causa de procesos simultáneos que crean instantáneas para el mismo sistema de archivos, AIX no consigue llevar a cabo las peticiones de eliminación. En los ejemplos anteriores, IBM Spectrum Protect anota un mensaje de aviso que solicita al usuario que elimine las instantáneas manualmente.

Procedimiento

Para suprimir una instantánea manualmente, emita los siguientes mandatos siguiendo el orden especificado:

1. `snapshot -q -c' ' <SRCFS>`
2. `df -k`
3. `unmount -f /tsm*`
4. `rmdir /tsm*`
5. `snapshot -d /dev/tsm*`

   Si el proceso de eliminación de instantáneas falla con el mensaje de error "Dispositivo ocupado" u otro mensaje de error, emita el mandato `- unmount -f <srcfs>` para desmontar el sistema de archivos de origen. A continuación, vuelva a intentar suprimir la instantánea.
6. `ls -l /dev/tsm*`

   Si permanecen los volúmenes lógicos `/DEV/TSM*` , emita el comando `- rmlv -f tsm*` .
7. Si tiene un sistema de archivo de origen desmontado, emita el comando `- mount <srcfs>` para montarlo.

Resultados

Si cualquiera de las instantáneas no se elimina durante un proceso de IBM Spectrum Protect anterior, IBM Spectrum Protect intenta eliminar las instantáneas durante la siguiente invocación, porque mientras permanezcan las instantáneas anteriores, AIX no podrá llevar a cabo las peticiones de eliminación de las instantáneas más recientes para un sistema de archivos determinado. Los siguientes casos indican cuándo IBM Spectrum Protect no intenta eliminar las instantáneas anteriores:

- Si la instantánea no se creó con IBM Spectrum Protect, IBM Spectrum Protect asigna un nombre con el prefijo "tsm" a sus instantáneas para distinguirlas de

otras instantáneas creadas para el mismo sistema de archivos. Si la instantánea no fue creada por IBM Spectrum Protect, se generará un mensaje de error que solicita al usuario que elimine la instantánea anterior y reintente la operación de nuevo.

- Si la instantánea fue creada por IBM Spectrum Protect pero todavía no está montada, la instantánea está siendo utilizada por otro proceso de IBM Spectrum Protect.
- Si la instantánea fue creada por IBM Spectrum Protect, no está montada, pero se acaba de crear, puede que la instantánea haya sido creada por otro proceso de IBM Spectrum Protect.

En todos estos casos, es posible que deba llevar a cabo una eliminación manual. Si existe cualquier instantánea anterior no utilizada, las copias de seguridad de IBM Spectrum Protect siguientes no conseguirán eliminar las instantáneas.

Importante: Existen arreglos de defectos de AIX relacionados con las instantáneas JFS2 AIX 6.1 o posterior. Si no se aplican los arreglos, puede producirse una caída del sistema AIX o IBM Spectrum Protect puede detenerse durante la eliminación de instantáneas y durante los procesos de consulta de instantáneas. También puede provocar daños en los datos durante la copia de seguridad de la imagen de bloques usados. Por lo tanto, , IBM Spectrum Protect no realizará las siguientes tareas:

- Supervisión de instantánea
- Supresión de instantánea

Para utilizar estas funciones, asegúrese de que el sistema operativo está al nivel AIX 6.1 o posterior.

Soluciones de soporte para la API de IBM Spectrum Protect

Existen recursos que le permitirán obtener información sobre la interfaz de programas de aplicación (API) de IBM Spectrum Protect o diagnosticarla.

La instrumentación de la API sólo se activará si la API `testflag INSTRUMENT:` está establecida en el archivo de configuración y se utilizan las llamadas **`dsmSetUp`** y **`dsmCleanUp`** en la aplicación.

Consulte *Uso de la interfaz de programación de la aplicación* o IBM Support Assistant para obtener más información.

Recopilación de información relacionada con la API antes de llamar al servicio de soporte de IBM

Puede ayudar de forma significativa a determinar un problema de interfaz de programas de aplicación (API) recopilando información acerca de su entorno.

Recopile el máximo de la información que figura a continuación antes de ponerse en contacto con el servicio de soporte de IBM:

- ¿En qué sistema operativo está experimentando el problema?
- ¿Cuál es el nivel exacto del sistema operativo, incluidos los service packs y los arreglos temporales aplicados?
- ¿Cuál es el nivel exacto de la API de IBM Spectrum Protect?
- ¿Cuál es el nivel exacto del servidor de IBM Spectrum Protect?

- ¿Cuál es la plataforma y el nivel del sistema operativo del servidor de IBM Spectrum Protect?
- ¿Cuál es el nivel exacto del agente de almacenamiento de IBM Spectrum Protect (si es un entorno fuera de LAN?
- ¿Cuál es la plataforma del agente de almacenamiento y el nivel del sistema operativo de IBM Spectrum Protect (si se trata de un entorno fuera de LAN)?
- ¿Qué aplicaciones se están ejecutando en el sistema?
- ¿Qué pasos son necesarios para recrear el problema? Si no puede recrear el problema, ¿qué pasos han causado el problema?

Recopilación de archivos de la API antes de llamar al servicio de soporte de IBM

La interfaz de programación de aplicaciones (API) de IBM Spectrum Protect crea los archivos de registro y otros datos importantes.

Reúna el mayor número de los siguientes archivos antes de ponerse en contacto conIBM Support:

- El archivo de anotaciones de error de la API de IBM Spectrum Protect. El archivo de registro de errores de la API predeterminado es `dsierror.log`.
- Cualquier archivo de rastreo que se crea para la API. Los distintivos de rastreo normales son `api`, `api_detail` o `verbdetail`.
- La salida de cualquier mandato u operación fallida que podría ser bien la salida de una consola que se redirige a un archivo a una imagen de pantalla actual del error.
- La salida del mandato **QUERY SYSTEM** del servidor.
- El archivo de registro de la actividad del servidor. El administrador de IBM Spectrum Protect puede ver este archivo de registro en nombre del usuario si este no dispone de un ID de usuario y de una contraseña de administrador de IBM Spectrum Protect.
- Si el cliente de la API está configurado para el traspaso de datos fuera LAN, recopile el archivo de opciones del agente de almacenamiento de IBM Spectrum Protect. El nombre predeterminado para el archivo de opciones es`dsmsta.opt`.
- Un programa o unas secciones breves del código fuente de la aplicación que invoquen a las llamadas de función de las API de IBM Spectrum Protect y que se sospeche que causan problemas.
- El archivo de opciones de la API de IBM Spectrum Protect.

  Los dos siguientes archivos de opciones se utilizan en sistemas operativos de Linux y UNIX:

  dsm.opt
  : El archivo de opciones de cliente

  dsm.sys
  : El archivo de opciones del sistema

  Para Windows, busque el archivo de opciones predeterminado `dsm.opt` o el archivo al que hace referencia la variable del entorno de **DSMI_CONFIG**. Para Linux and UNIX, el archivo de opciones predeterminado es `dsm.sys` y se encuentra en el directorio al que hace referencia la variable de entorno de **DSMI_DIR**.

  En otros sistemas operativos, el archivo de opciones del cliente `dsm.opt` contiene todas las opciones. Las siguientes definiciones son variables de entorno que

describen la ubicación de los archivos de opciones y otros componentes de la interfaz de programación de aplicaciones:

DSMI_CONFIG
El nombre completo para el archivo de opciones de cliente.

DSMI_DIR
Los puntos de variable *DSMI_DIR* al directorio de instalación de API y solo se utiliza para encontrar el archivo`dsm.sys` en Linux and UNIX. Cuando esté configurado *DSMI_DIR* asegúrese de que haya un archivo `dsm.sys` en el mismo directorio.

DSMI_LOG
La variable *DSMI_LOG* apunta a la vía de acceso correspondiente al archivo `dsierror.log`. Si está configurada la opción de cliente `errorlogname`, la ubicación que especifica la opción sustituye al directorio que especifica *DSMI_LOG*.

Consejo: Si la variable *DSMI_LOG* apunta a un directorio para el que el usuario no tiene permisos de grabación, **`dsmSetup`** y**`dsmInitEx`** fallan con el código de retorno `DSM_RC_ACCESS_DENIED (106)`.

Si la opción `errorlogname` se define en el archivo de opciones `dsm.sys/dsm.opt`, su valor se utiliza como el nombre de registro de error en vez del valor predeterminado`dsierror.log`.

Comprobar de que la API utiliza el archivo de opciones correcto

AIX Linux Mac OS X

Cuando recopile archivos de la interfaz de programas de aplicación (API), debe comprobar que la API utiliza el archivo de opciones o la stanza del servidor correctos en el archivo `dsm.sys`.

Procedimiento

Complete estos pasos para verificar que la API utiliza el archivo de opciones o la stanza del servidor correctos:

1. Inserte una opción o un valor erróneo en el archivo de opciones de cliente o la stanza de servidor en `dsm.sys`. Por ejemplo, si no está claro si la API utiliza el servidor `srvr1.cmpron`, inserte la sentencia 'ERRONEOUS_OPTION 12345' en la stanza de servidor `srvr1.cmpron` del archivo `dsm.sys`. Consulte el ejemplo siguiente:

```
...
SERVERNAME srvr1.cmproff
COMPRESSION NO
TCPSERVERADDRESS computer.company.com

SERVERNAME srvr1.cmpron
COMPRESSION YES
ERRONEOUS_OPTION 12345
TCPSERVERADDRESS computer.company.com

SERVERNAME srvr1.pwdfl
PASSWORDACCESS GENERATE
PASSWORDDIR .
TCPSERVERADDRESS computer.company.com
...
```

2. Compruebe que la API detecta el error. Puede utilizar el programa de API de muestra, `dapismp`, con este objetivo.

```
# dapismp
...
Enter selection ==>0
Node name:node1
Owner name:
Password:
API Config file:
Session options:
User Name:
User pswd:
Are the above responses correct (y/n/q)?
Doing signon for node node1, owner, with password
*** Init failed: ANS0220E (RC400)  Se ha encontrado una opción que no es
   válida durante el análisis de opciones.
```

   Si no se informa de ningún error, se actualizó el archivo de opciones erróneas.
3. Compruebe los valores de la variable del entorno que se mencionaron en "Recopilación de archivos de la API antes de llamar al servicio de soporte de IBM" en la página 37 o repita los pasos 1 y 2 con un archivo de opciones o una stanza de servidor diferente.
4. Elimine la opción insertada en el paso 1.

Cómo determinar si los datos se envían al agente de almacenamiento en lugar de al servidor

Debe saber si los datos se envían al agente de almacenamiento de IBM Spectrum Protect en lugar de a un servidor. Si los datos se envían al agente de almacenamiento, no podrá recuperarlos.

Procedimiento

Complete los pasos siguientes para verificar que los datos se envían al agente de almacenamiento de IBM Spectrum Protect en lugar de al servidor:

1. Añada las opciones de rastreo siguientes al archivo de opciones del cliente antes de realizar una copia de seguridad o archivar los objetos:
   - `TRACEFILE <nombre_archivo_rastreo>`
   - `TRACEFLAGS api api_detail verbdetail`
2. Examine el archivo de rastreo tras la operación y encuentre una sentencia similar a la siguiente:

   ```
   dsmSendObj ENTRY:... objNameP: '<nombre_archivo>'
   ```

   Esta sentencia va seguida de la siguiente sentencia de rastreo:

   ```
   tsmEndSendObjEx: Total bytes sent * *, encryptType is *** encryptAlg is
   *** compress is *, totalCompress is * * totalLFBytesSent * *
   ```

   La sentencia de rastreo indica si el objeto **totalLFBytesSent** se envió al agente de almacenamiento de IBM Spectrum Protect. Si **totalLFBytesSent** es 0 0, los datos se envían directamente al servidor de IBM Spectrum Protect.

   O bien puede ser la propia aplicación la que determine si los datos se han enviado a través de una vía de acceso fuera de la LAN utilizando la llamada a función **dsmEndSendObjEx** y la estructura de datos **dsmEndSendObjExOut_t**.

   ```
   /*------------------------------------------------------------------------+
   |  Definición de tipo para dsmEndSendObjExOut_t
   +------------------------------------------------------------------------*/
   typedef struct dsmEndSendObjExOut_t
   ```

```
{
dsUint16_t     stVersion; /* structure version */
dsStruct64_t       totalBytesSent;      /* total bytes read from app */
dsmBool_t          objCompressed;       /* was object compressed */
dsStruct64_t   totalCompressSize;  /* total size after compress */
dsStruct64_t   totalLFBytesSent;  /* total bytes sent LAN Free */
dsUint8_t          encryptionType;      /* type of encryption used   */
 }dsmEndSendObjExOut_t;
 totalLFBytesSent - The total LAN-free bytes that were sent.
```

Por ejemplo:

```
...
    rc = dsmEndSendObjEx(&endSendObjExIn, &endSendObjExOut);
    if (rc)
 {
     printf("*** dsmEndSendObjEx failed: ");
     rcApiOut(dsmHandle, rc);
 }
 else
 {
     dI64toCh(&endSendObjExOut.totalLFBytesSent,t,10);
     format_number(t,t2);
     printf("LAN-free bytes sent: %s\n", t2);
```

Qué hacer a continuación

Consulte *Llamadas a función de la API* en *Utilización de la interfaz de programación de aplicaciones* para obtener más detalles.

Cómo ejecutar aplicaciones que utilizan la API como ID de usuario no root

AIX Linux Mac OS X

Debe realizar pasos específicos si tiene sesión iniciada con ID de usuario que no es root que intenta ejecutar una aplicación que utiliza la interfaz de programación de aplicaciones (API).

Procedimiento

Complete los pasos siguientes para permitir que un ID usuario no root acceda a la API:

1. Establezca la variable de entorno **DSMI_CONFIG**. Compruebe que el ID usuario no root cuenta con permiso de lectura para el archivo de opciones del cliente especificado por DSMI_CONFIG. Si no, dsmInit/dsmInitEx falla con el código de retorno DSM_RC_NO_OPT_FILE (406). Por ejemplo, el siguiente archivo de opciones es ilegible para un ID de usuario no root; en consecuencia, deben actualizarse los permisos del archivo:

   ```
   $ ls -l $DSMI_CONFIG
   -rwx------   1 root  sys  86 Oct 7 13:07 /testfsapi/callmt_nr/dsm.opt
   $ su root
   Password:
   # chmod a+r /testfsapi/callmt_nr/dsm.opt
   # exit
   $ ls -l $DSMI_CONFIG
   -rwxr--r--   1 root  sys  86 Oct 7 13:07 /testfsapi/callmt_nr/dsm.opt
   ```

2. Establezca la variable de entorno **DSMI_DIR** en el directorio de instalación de la API. Compruebe que el ID de usuario no root cuenta con permiso de lectura para el archivo de opciones del sistema especificado por $DSMI_DIR/dsm.sys.

```
$ export DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
$ ls -l $DSMI_DIR/dsm.sys
-rw-r--r--   1 root  sys
4712 Oct 19 18:07 /opt/tivoli/tsm/client/api/bin64/dsm.sys
```

3. Establezca la variable de entorno **DSMI_LOG**. Compruebe que el ID de usuario no root tiene permiso de grabación para este directorio. Por ejemplo, el directorio siguiente DSMI_LOG es propiedad de un ID de usuario distinto de root:

   ```
   $ ls -ld $DSMI_LOG
   drwxr-xr-x  2 apitest  users   96 Oct 19 17:56 /testfsapi/callmt_nr/logs
   ```

   Si **PASSWORDACCESS GENERATE** se establece en el archivo de opciones del sistema dsm.sys, realice los pasos 4 y 5, si no, vaya al paso 6.

4. Opcional: Compruebe la propiedad y los permisos del Agente de comunicaciones de confianza (TCA) solo si la opción PASSWORDDIR no se utiliza o si apunta a un directorio que en el que el usuario no tiene permisos de lectura o grabación. Este archivo se encuentra en el directorio indicado por la variable de entorno **DSMI_DIR**. Por ejemplo, el siguiente TCA dispone de la propiedad y los permisos correctos:

   ```
   $ ls -l $DSMI_DIR/dsmtca
   -rwsr-xr-x 1 root bin 5021160 Oct 14 09:48
   /opt/tivoli/tsm/client/api/bin64/dsmtca
   ```

   Unos permisos o una propiedad incorrecta resultan en un DSM_RC_AUTH_FAILURE (137) devuelto por parte de dsmInit. De forma adicional, es necesario que utilice la misma versión de la biblioteca de API y dsmtca. Con versiones distintas, aparecen errores.

   ```
   Error : calling program and dsmtca are not compatible
   calling program build date :  Mon Oct 18 21:15:59 2004  Mon Oct 18 21:15:59 2004
   TCA build date             :  Wed Oct 13 16:48:03 2004  Wed Oct 13 16:48:03 2004
   *** Init failed: ANS0282E (RC168)  El archivo de contraseñas no está disponible.
   ```

5. El usuario root debe generar el archivo de contraseña TSM.PWD utilizando el cliente de archivado y copia de seguridad o la aplicación API de ejemplo **dapismp**. Un usuario autorizado es cualquier ID de usuario no raíz que tenga acceso de lectura y grabación en la contraseña guardada (archivo TSM.PWD). La ubicación del archivo de contraseña la determina la opción PASSWORDDIR del archivo de opciones del sistema dsm.sys. En el siguiente ejemplo, la aplicación de prueba de la API genera el archivo de contraseña TSM.PWD para un nodo cuya contraseña es *oddesy*:

```
# dapismp
********************************************************************************
* Welcome to the sample application for the IBM Spectrum Protect API. *
* API Library Version = 5.4.0.0 *
********************************************************************************
Choose one of the following actions to test:
0.  Signon
1.  Backup
2.  Restore
3.  Archive
4.  Retrieve
5.  Queries
6.  Change Password
7.  Utilities : Deletes, Updates, Logevent, SetAccess, RetentionEvent
8.  Set preferences, envSetUp
9.  Exit to system
10. Restore/Retrieve Without Offset Prompt
11. Extended Signon
Enter selection ==>0
Node name:
Owner name:
Password:oddesy
API Config file:
Session options:
User Name:
User pswd:
Are the above responses correct (y/n/q)?
Doing signon for node, owner, with password oddesy
Handle on return = 1
Choose one of the following actions to test:
0.  Signon
1.  Backup
2.  Restore
3.  Archive
4.  Retrieve
5.  Queries
6.  Change Password
7.  Utilities : Deletes, Updates, Logevent, SetAccess, RetentionEvent
8.  Set preferences, envSetUp
9.  Exit to system
10. Restore/Retrieve Without Offset Prompt
11. Extended Signon
Enter selection ==>9
# ls -l TSM.PWD
-rw-------   1 root       sys            121 Oct 19 18:28 TSM.PWD
Function call dsmInit returns DSM_RC_NO_PASS_FILE (168), if the password
file is not present in the directory specified by the PASSWORDDIR option.
```

6. Si el programa de utilidad de rastreo está activado, compruebe que el ID de usuario no root tiene permiso de grabación para el archivo indicado emitiendo la opción TRACEFILE.

Determinación de problemas de copia de seguridad basada en el registro por diario

Windows

La copia de seguridad basada en el registro por diario (JBB) es adecuada para realizar copias de seguridad de sistemas de archivos con pequeñas o moderadas cantidades de actividad de modificaciones entre ciclos de copia de seguridad.

Cómo determinar si una copia de seguridad tendrá diario

Windows

Antes de implementar una copia de seguridad, debe determinar si ésta será con diario.

Acerca de esta tarea

Para asegurarse de que la copia de seguridad es con diario, siga estos pasos:

Procedimiento

1. Configure el daemon de diario para registrar por diario el sistema de archivos del que se está realizando una copia de seguridad. El daemon de diario incluye en el registro un sistema de archivos cuando se lista el sistema de archivos en el archivo de configuración `tsmjbbd.ini`. Consulte la información de configuración siguiente:

   ```
   [JournaledFileSystemSettings]
   ;
   ; Lista de sistemas de archivos registrados
   JournaledFileSystems=c:
   ```

2. Realice una copia de seguridad incremental completa del sistema de archivos correspondiente mientras se realiza un registro del sistema de archivos de forma activa. Esta copia de seguridad incremental completa debe establecer la fecha de "finalización de la última copia de seguridad" en el espacio de archivos del servidor IBM Spectrum Protect para que el diario se establezca como válido. Puede ver la fecha de "finalización de la última copia de seguridad"" si emite el mandato del servidor **QUERY FILESPACE**. Después de que el diario se establezca como válido, las copias de seguridad posteriores por el mismo nodo en el mismo servidor serán con diario. Si una copia de seguridad utiliza un nodo o un servidor distintos, la copia de seguridad no tendrá diario, pero el diario seguirá siendo válido para el nodo y el servidor originales, y las copias de seguridad del nodo y el servidor originales tendrán diario.

   El siguiente mensaje es un ejemplo de lo que se graba en el Registro de eventos de aplicación de Windows cuando un diario se establece inicialmente como válido:

   ```
   Journal set to valid for fs 'H:' and will be used for backup by
   node GSHLAGER3 to server GSHLAGER2_SERVER1.
   ```

3. Compruebe que el servidor y el nodo de IBM Spectrum Protect que utiliza la copia de seguridad coincidan con el nodo y el servidor para el que el diario es válido.

4. También puede utilizar el programa de utilidad de visualización de base de datos con diario para determinar el estado actual de un diario. Si se reinicia un diario válido, las copias de seguridad no serán con diario hasta que éste se vuelva a validar.

   El mensaje siguiente se graba en el Registro de eventos de aplicación de Windows cuando se reinicia un diario:

   ```
   Journal database 'c:\tsmjournal\tsmH__.jdb' for fs 'H:' has been
   deleted and reset to the invalid state.
   ```

Reinicio de un diario válido

AIX Linux Windows

Puede aumentar el rendimiento reiniciando un diario válido.

Los motivos para reiniciar un diario válido:

- Condiciones de error en el daemon de diario
  - Errores de desbordamiento de almacenamiento intermedio producidos por una excesiva actividad de modificaciones en el sistema de archivos de diario que se está supervisando para las modificaciones
  - Errores de acceso en la base de datos de diario (errores de disco lleno, etc.)
- Solicitud por un cliente de copia de seguridad
- Los clientes emitirán una petición de reinicio del diario cuando se determine que un sistema de archivos de diario presenta un error de integridad por una de las siguientes razones:
  - El espacio de archivos del servidor ya no existe
  - El espacio de archivos del servidor se ha suprimido después de la última copia de seguridad
  - El juego de políticas del nodo se actualizó después de la última copia de seguridad
  - Las fechas de finalización de última copia de seguridad o de inicio de última copia de seguridad no son válidas (no están establecidas)

Ejecución del daemon de diario en primer plano

Windows

Puede mejorar las posibilidades de diagnóstico y la capacidad de prueba ejecutando el daemon de diario en primer plano, en lugar de como un servicio de Windows.

Inicie el daemon de diario desde un indicador de mandatos de Windows como se indica a continuación: `tsmjbbd.exe i`

El programa de utilidad de visualización de base de datos con diario

Windows

El programa de utilidad de visualización de base de datos con diario proporciona información valiosa para ayudar en la determinación de problemas de las copias de seguridad con registro por diario.

El programa de utilidad de visualización de base de datos con diario proporciona la siguiente información:

- El estado actual del diario
- El sistema de archivos del que realiza el seguimiento el diario
- Indicación de la hora de activación del diario
- Indicación de la hora de validación del diario
- El tamaño máximo admitido del diario
- El nodo y el servidor para los que es válido el diario
- El número de entradas que hay actualmente en el diario

Nota: En clientes de archivado y copia de seguridad posteriores a la versión 6.3.1, no puede visualizar el contenido de los diarios abiertos con el programa de utilidad de visualización. Un diario abierto es el diario que abre actualmente otro proceso, tal como el daemon de diario. Sin embargo, puede ver el contenido del registro de control de diario abierto. El programa de utilidad de visualización está disponible con V6.3.1 y con clientes de copia de seguridad y archivado más recientes. Para obtener más información acerca del programa de utilidad de visualización, consulte la siguiente nota técnica: Ejecución del programa de utilidad dbviewb.exe en modalidad por lotes.

Este programa de utilidad también permite buscar, insertar o eliminar entradas concretas de una base de datos de diario.

La sintaxis de este programa de utilidad es:

```
dbviewb <nombre_completo_archivo_base_datos_diario>
dbviewb <nombre_completo_archivo_base_datos_diario> <i>
```

```
D:\tsm540c\debug\bin\winnt_unicode>dbviewb c:\tsmjournal\tsmh__.jdb
IBM Spectrum Protect
Journal Database Viewing Utility
Version 5, Release 4, Level 0.0
Last Update: Nov 28 2006
Querying Journal DB ...
Journal Database Information:
Database File           c:\tsmjournal\tsmh__.jdb
Database File Disk Size 81 KB (83754 Bytes)
Journal  File System    H:
Journal Activation Date Tue Nov 28 11:49:05 2006
Journal Validation Date Wed Nov 29 16:41:11 2006
Maximum Journal Size    8191 PB (9223372036854775807 Bytes)
Journal Type            Change Journal
Journal State           Valid
Valid for Server        GSHLAGER2_SERVER1
Valid for Node          GSHLAGER3
Number of DB Entries    22
D:\tsm540c\debug\bin\winnt_unicode>
```

```
D:\tsm540c\debug\bin\winnt_unicode>dbviewb c:\tsmjournal\tsmh__.jdb i
IBM Spectrum Protect
Journal Database Viewing Utility
Version 5, Release 4, Level 0.0
Last Update: Nov 28 2006
Querying Journal DB ...
Journal Database Information:
Database File           c:\tsmjournal\tsmh__.jdb
Database File Disk Size 81 KB (83754 Bytes)
Journal  File Syst em   H:
Journal Activation Date Tue Nov 28 11:49:05 2006
Journal Validation Date Wed Nov 29 16:41:11 2006
Maximum Journal Size    8191 PB (9223372036854775807 Bytes)
Journal Type            Change Journal
Journal State           Valid
Valid for Server        GSHLAGER2_SERVER1
Valid for Node          GSHLAGER3
Number of DB Entries    22
Especifique la solicitud en una única línea, con el siguiente formato:
Tipo solicitud [clave entrada]
"Tipo solicitud" puede ser uno de los siguientes:
Del     Eliminar una fila de la base de datos. Se necesita el nombre
de archivo sensible a las mayúsculas y minúsculas totalmente calificado.
Find    Buscar la entrada cuya clave es el argumento.
List Imprimir todas las entradas en stdout. No se necesita ningún argumento.
Quit    Salir
Please enter your request: find H:\dbview.example\Dir3Depth1\F2.txt
Located Journal Database Record:
```

```
----------------------------------------
Object Name  : H:\dbview.example\Dir3Depth1\F2.txt
Action       : Modify
Object Type  : File
Inserted : Fri Dec 01 10:15:28 2006
Object Time : Fri Dec 01 14:15:28 2006
Hit Count    : -2110169276
----------------------------------------
Please enter your request: quit
```

Utilización de servicios de duplicación de volúmenes de Windows

Windows

El cliente de IBM Spectrum Protect Windows utiliza los servicios de duplicación de volúmenes (VSS) para completar la copia de seguridad de estado del sistema y los servicios del sistema. VSS también puede utilizarse como un proveedor de instantáneas para el soporte de archivos abiertos (OFS) y las operaciones de imágenes en línea.

Definición de errores transitorios de VSS

Windows

El cliente considera que múltiples errores del Servicio de duplicación de volúmenes (VSS) son transitorios. Los errores transitorios son errores de red o unidades que se comportan de manera incorrecta y que puede que requieran una recuperación de copia de seguridad.

Cuando aparece uno de estos errores, el cliente, de forma predeterminada, reintentará el proceso de copia de seguridad de VSS tres veces a intervalos de 30 segundos. El número de reintentos y el intervalo entre ellos se pueden configurar mediante dos indicadores de prueba (**TESTFLAG SETVSSMAXRETRY** y **TESTFLAG SETVSSDELAY**). El cliente considera como transitorios los siguientes errores VSS:

VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED
VSS_E_SNAPSHOT_SET_IN_PROGRES
VSS_E_MAXIMUM_NUMBER_OF_SNAPSHOTS_REACHED
VSS_E_PROVIDER_VETO VSS_E_UNEXPECTED
VSS_E_FLUSH_WRITES_TIMEOUT
VSS_E_HOLD_WRITES_TIMEOUT
VSS_E_WRITERERROR_TIMEOUT
VSS_E_WRITERERROR_RETRYABLE
VSS_E_WRITERERROR_OUTOFRESOURCES
VSS_E_WRITER_NOT_RESPONDING
VSS_E_VOLUME_IN_USE
VSS_E_PROVIDER_IN_USE
VSS_E_UNEXPECTED_PROVIDER_ERROR
VSS_E_UNEXPECTED_WRITER_ERROR

Definición de los indicadores de prueba de Windows VSS

Windows

El cliente utiliza dos indicadores de prueba distintos para configurar el número de intentos del servicio de duplicación de volúmenes (VSS) y el intervalo entre intentos.

Los siguientes indicadores de prueba se utilizan para establecer el número de intentos de IBM Spectrum Protect y el intervalo entre ellos:

SETVSSMAXRETRY
Especifica el número de veces que se reintenta el proceso de copia de seguridad VSS si se produce un error transitorio. El valor predeterminado es reintentarlo tres veces.

SETVSSDELAY
Especifica el número de segundos que se esperan entre reintentos del proceso de copia de seguridad de VSS, en el caso de que se produzca un error transitorio. El valor predeterminado es 60 segundos.

Ejemplo de archivo de opción:

```
retry 10 times at 300 second intervals
TESTFLAG SETVSSMAXRETRY:10
TESTFLAG SETVSSDELAY:300
```

Ajuste de servicios de duplicación de volúmenes

Windows

Hay varios arreglos disponibles para el Servicio de duplicación de volúmenes (VSS) de Microsoft si experimenta dificultades con el ajuste de VSS.

Control del tamaño de área de diferencia de VSS

Después de aplicar esos arreglos, aparece uno de los siguientes eventos:

- "The shadow copy of volume C: took too long to install"
- "The shadow copy of volume C: was stopped because the diff area file could not grow in time."

Reduzca la carga de E/S en este sistema para evitar estos problemas. Si siguen apareciendo los eventos, utilice la siguiente clave de registro para controlar el tamaño del área de diferencia utilizada por VSS:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VolSnap\ MinDiffAreaFileSize : REG_DWORD: <`*`tamaño_MB`*`>` (el tamaño predeterminado es 300, pero se puede incrementar hasta 3000).

Tamaño máximo del registro de sucesos

Microsoft indica que si las anotaciones de eventos son suficientemente grandes, la operación de copia puede superar el tiempo de espera de los sistemas con una carga elevada de E/S o una carga de memoria elevada. Es mejor que el tamaño del registro sea inferior a 64 MB.

Recopilación de información de diagnóstico de VSS para el servicio de asistencia de Microsoft

Windows

La información de diagnóstico de IBM para fallos de Servicios de duplicación de volúmenes (VSS) puede no ser la que necesita. Puede encontrar información de diagnóstico para fallos de VSS desde el sitio de soporte de Microsoft.

Si el error de VSS está fuera del ámbito de IBM Spectrum Protect, recopile la información siguiente para la asistencia de Microsoft:

- Registro de eventos de aplicación de Windows
- Registro de eventos del sistema de Windows
- rastreo VSS

Examine los archivos de registro de eventos de aplicación y del sistema, centrándose en los eventos de error creados por las fuentes VolSnap y VSS en el momento del error. Puede extraer de las anotaciones los eventos vinculados para identificar el problema y lograr una interacción más productiva con el soporte de Microsoft.

Resolución de errores con el rastreo VSS

Windows

Puede resolver los errores del Servicio de duplicación de volúmenes (VSS) realizando un rastreo VSS.

Acerca de esta tarea

Siga estos pasos para realizar un rastreo VSS:

Procedimiento

1. Cree un archivo `tracing.reg` y cambie la entrada TraceFile para indicar un volumen que no tendrá creada una copia de duplicación. Utilice el contenido de la parte inferior de este archivo para crear el archivo. Tenga en cuenta el uso del delimitador de barra invertida doble; debe especificar "`\\`" como delimitador de cada barra invertida en la vía de acceso que desea especificar.
2. Pulse dos veces en el archivo desde dentro de Windows Explorer para instalar `tracing.reg`.
3. Reproduzca el problema.
4. Desactive el rastreo eliminando la clave "`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing`".

Resultados

El archivo de registro `tracefile.reg` muestra el siguiente contenido:

```
Windows Registry Editor Versión 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing]
"TraceFile"="c:\\trace.txt"
"TraceLevel"=dword:ffffffff
"TraceEnterExit"=dword:00000001
"TraceToFile"=dword:00000001
"TraceToDebugger"=dword:00000000
"TraceFileLineInfo"=dword:00000001
"TraceForceFlush"=dword:00000000
```

Ejecución de llamadas VSS API con el programa de ejemplo vsreq.exe

Windows

El Software Developers's Kit (SDK) del Servicio de duplicación de volúmenes contiene el programa de ejemplo **vsreq** (solicitante de VSS). El programa solicitante de VSS efectúa una secuencia de llamadas a la API de VSS como las llamadas que efectúa el cliente de archivado y copia de seguridad.

Puede compilar y ejecutar `vsreq.exe` en el sistema que ha fallado para determinar si **vsreq** y IBM Spectrum Protect encuentran el mismo problema. Si **vsreq** puede reproducir el mismo problema que IBM Spectrum Protect, la salida de **vsreq** se puede facilitar al servicio de soporte de Microsoft para ayudar en el diagnóstico del problema de VSS.

En algunos casos, Microsoft proporcione una herramienta de análisis del subsistema de entrada/salida (E/S) ("yapt") para recopilar datos del rendimiento de E/S para el análisis. **vshadow** es una herramienta que también está disponible como alternativa a **vsreq**.

Comparación de la interacción de IBM Spectrum Protect y Ntbackup.exe con VSS

Windows

Cuando se utiliza el archivo ejecutable `Ntbackup.exe`, no se aprovechan al máximo los Servicios de duplicación de volúmenes (VSS) y no siempre puede considerarse como punto de referencia para la interacción de IBM Spectrum Protect con VSS.

La diferencia conocida entre `Ntbackup.exe` y IBM Spectrum Protect en el contexto de VSS es que `Ntbackup.exe` no utiliza VSS para realizar la copia de seguridad de Active Directory (NTDS). Aunque `Ntbackup.exe` utiliza VSS para realizar una instantánea, sigue utilizando la API de copia de seguridad heredada de NTDS para leer datos del disco. IBM Spectrum Protect utiliza la interfaz de VSS para leer datos NTDS del disco. Si hay algún problema con el responsable del grabador de VSS para NTDS, no se revelará con `Ntbackup.exe`.

Emita el mandato **VSSADMIN LIST** para consultar el estado del escritor de VSS para garantizar que VSS se encuentra en un estado de estable o preparado.

Mandatos `SHOW` para el cliente de archivado y copia de seguridad

Los mandatos **SHOW** son mandatos de diagnóstico no admitidos que se utilizan para mostrar información sobre estructuras de control en memoria y otros atributos de tiempo de ejecución. Los mandatos **SHOW** los utilizan el desarrollo y el servicio sólo como herramientas de diagnóstico. Hay varios mandatos **SHOW** para el cliente de copia de seguridad/archivado.

Según la información que muestre un mandato **SHOW**, puede haber casos en los que la información cambie o casos en los que puede hacer que la ejecución de la aplicación (cliente, servidor o agente de almacenamiento) se detenga. Los mandatos **SHOW** deben utilizarse solo cuando el personal de desarrollo o servicio lo sugieran. Los mandatos **SHOW** incluidos en la tabla Tabla 3 en la página 50 no son todos los mandatos **SHOW** disponibles.

Tabla 3. Mandatos SHOW para el cliente de archivado y copia de seguridad

Mandato SHOW	Descripción	Información
CLUSTER	Muestra información sobre asignaciones de disco en Microsoft Cluster.	Esto es útil para mostrar información sobre la (configuración de) asignación de disco en un entorno Microsoft Cluster.
DOMAIN	Muestra información sobre los dominios configurados para utilizarse para procesos de copia de seguridad incrementa.	Útil para mostrar y resumir las opciones de cliente `DOMAIN`, `DOMAIN.IMAGE` y `DOMAIN.NAS`.
OPTIONS	Muestra las opciones de cliente.	Resulta útil para determinar los valores de las opciones de cliente.
OPTTABLE	Muestra información sobre las opciones administradas por el servidor en contraposición a las gestionadas por el archivo de opciones de cliente.	El cliente puede recibir sus valores de opciones tanto del archivo de opciones de cliente como del servidor. Para recibir la opción del servidor, debe definirse un conjunto de opciones de cliente utilizando el mandato **`DEFINECLOPTSET`**. Este mandato le ayuda a determinar si el cliente utiliza una opción configurada desde el archivo de opciones o una opción configurada desde un conjunto de opciones de cliente definido en el servidor.
PLUGINS	Muestra información sobre los complementos para este cliente.	El cliente utiliza complementos para ofrecer capacidades adicionales, como copia de seguridad de imagen. Este mandato **`SHOW`** muestra los complementos instalados para este cliente y los atributos de los diversos complementos; por ejemplo, su versión, tipo y ubicación.
SESSION	Muestra las capacidades que este cliente puede tener para esta conexión al servidor.	El cliente y de servidor negocian e informan sobre las capacidades que posee cada uno de ellos cuando un cliente o un servidor inicia una sesión. Este mandato **`SHOW`** informa de las posibilidades disponibles para este servidor y cliente.
SYSTEMSTATE	Para los clientes de Windows, muestra los datos de **`SYSTEM STATE`** disponibles en este cliente.	El mandato **`SHOW`** de SYSTEMSTATE es útil para determinar los archivos **`SYSTEM STATE`** instalados en este sistema Windows y los archivos de los que se puede realizar una copia de seguridad.

Tabla 3. Mandatos SHOW para el cliente de archivado y copia de seguridad (continuación)

Mandato SHOW	Descripción	Información
TRACEFLAGS	Muestra información sobre clases de rastreo y clases de rastreo agregadas para este cliente.	El mandato **SHOW** de TRACEFLAGS es útil para determinar qué clases de rastreo y las clases de rastreo agregadas se pueden utilizar para este cliente.
VERSION	Muestra la versión y la fecha de compilación para este cliente.	El mandato **SHOW** de VERSION es útil para determinar qué cliente se está ejecutando y cuándo se compiló.

Resolución de problemas para realizar la recuperación de las bases de datos SQL individuales deMicrosoft desde una copia de seguridad de la máquina virtual

Windows

Puede utilizar IBM Spectrum Protect for Virtual Environments Data Protection for VMware para recuperar las bases de datos de SQL individuales de Microsoft desde una copia de seguridad de la máquina virtual. Cuando recupera una base de datos, es posible que debas solucionar problemas comunes que puedan ocurrir con las bases de datos SQL individuales.

Cuando utiliza la protección de la aplicación autocontenida paraMicrosoft SQL en Data Protection for VMware, puede realizar una copia de seguridad de una máquina virtual que alberga una aplicación deMicrosoft SQL Server. Si desea restaurar una base de datos SQL de Microsoft desde una copia de seguridad de una máquina virtual, debe utilizar IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server.

La siguiente tabla contiene soluciones a problemas comunes que puede encontrar cuando intente recuperar las bases de datos de Microsoft SQL desde una copia de seguridad de una máquina virtual.

Tabla 4. Información de resolución de problemas para recuperar las bases de datos individuales de Microsoft SQL desde una copia de seguridad de la máquina virtual

Problema	Solución o explicación
No se puede acceder a las copias de seguridad de la base de datos de Data Protection for SQL.	"Resolución de problemas de acceso a base de datos" en la página 52
Puede ver solo las copias inactivas de las bases de datos de SQL cuando utilice la GUI de Data Protection for SQL o el mandato **tdpsqlc**.	"Vista de las copias activas de las bases de datos de Microsoft SQL" en la página 53
No pude ver los nombres de la base de datos de SQL que contienen caracteres desde el conjunto de caracteres de doble bytes (DBCS) con Data Protection for SQL.	"Bases de datos Microsoft SQL con nombres DBCS" en la página 54
Puede utilizar la protección de la aplicación durante una copia de seguridad de la máquina virtual y ha recibido avisos o mensajes de error.	"Respuesta a mensajes de copias de seguridad de máquina virtual con protección de la aplicación" en la página 54

Tabla 4. Información de resolución de problemas para recuperar las bases de datos individuales de Microsoft SQL desde una copia de seguridad de la máquina virtual (continuación)

Problema	Solución o explicación
Desea determinar qué bases de datos SQL estaban en la máquina virtual invitada cuando se realizó una copia de seguridad de la máquina virtual.	"Guardar los archivos de manifiesto VSS XML" en la página 55
Desea ver el estado de los grabadores VSS sin la máquina virtual invitada.	"Determinar si una copia de seguridad de una máquina virtual puede fallar" en la página 56

Resolución de problemas de acceso a base de datos

Windows

Si ha realizado una copia de seguridad de una máquina virtual huésped que aloja una aplicación de Microsoft SQL Server, es posible que no pueda acceder a las bases de datos con Data Protection for SQL.

Procedimiento

Para resolver los problemas de acceso a base de datos, siga estos pasos:

1. Verifique que la protección de la aplicación se utilizó cuando creó la copia de seguridad de máquina virtual:
   a. En la ventana Indicador de mandatos, emita el siguiente mandato del cliente de copia de seguridad/archivado para visualizar la lista de copias de seguridad de máquina virtual correctas en el servidor:

      ```
      dsmc -node=datacenter_node query vm vm_name -detail
      ```

      Donde*datacenter_node* es el nombre de nodo de la máquina virtual que aloja los datos en el centro de datos y *vm_name* es el nombre de la máquina virtual de la que ha realizado la copia de seguridad.
   b. Verifique la salida de este mandato contiene los siguientes cambios de salida:

      ```
      application protection type: 'TSM VSS'
      application(s) protected:    'MS SQL 2008 – database-level recovery'
      ```

      Si la salida no contiene los campos de salida, el segundo campo no incluye el texto `database-level recovery`, complete los pasos siguientes:
      1) Asegúrese de que el cliente de archivado y copia de seguridad de V7.1 o superior esté instalado en el transportador de datos y de que el archivo de opciones del cliente contiene la opción `include.vmtsmvss nombre_máquina_virtual`.
      2) Realice una copia de seguridad de la máquina virtual de nuevo.
2. Verifique que el nombre del equipo de la máquina virtual del invitado no se ha modificado después de crearse la copia de seguridad de la máquina virtual.
3. Verifique que el nodo de DSMAGENT del invitado tiene acceso a las copias de seguridad de la máquina virtual del nodo del centro de datos.
   a. Emita el siguiente mandato para verificar que el nodo de cliente tiene acceso a las versiones de copia de seguridad de la máquina virtual en el servidor:

```
dsmc –node=datacenter_node query access
```

Donde *datacenter_node* es el nombre del nodo virtual que aloja los datos en el centro de datos.

b. Verifique que la salida del mandato contiene los siguientes campos:

```
Type     Node            User   Path
----     ----------------------------------------
Backup   dsmagent_node   *      \VMFULL-vm_name\*\*
```

Si la salida no contiene esta información, vuelva a ejecutar el mandato **set access** en el nodo transportador de datos que el nodo DSMAGENT acceda a las copias de seguridad de la máquina virtual del invitado. Por ejemplo, emita el siguiente mandato:

```
dsmc set access backup –type=vm dsmagent_node vm_name
```

Donde*dsmagent_node* es el nombre de nodo del cliente de archivado y copia de seguridad del invitado de la máquina virtual,y *vm_name* es el nombre de la máquina virtual de la que ha realizado la copia de seguridad.

Qué hacer a continuación

Acceda a las bases de datos individuales con Data Protection for SQL de nuevo.

Vista de las copias activas de las bases de datos de Microsoft SQL

Windows

Para poder visualizar las copias activas de las bases de datos de Microsoft SQL con Data Protection for SQL, debe ejecutar todas las copias de seguridad primarias y subsecuentes incrementales de las base de datos SQL mediante Data Protection for VMware con la protección de la aplicación.

Si se utiliza la protección de la aplicación para la copia de seguridad primaria de las bases de datos de Microsoft SQL, pero no utilizó la protección de la aplicación para las copias de seguridad incrementales subsecuentes, no se pueden utilizar las copias de seguridad activas válidas para las operaciones de restauración de la base de datos SQL individuales. Data Protection for SQL examina la copia de seguridad de la máquina virtual y puede mostrar solo las bases de datos SQL desde las copias de seguridadde la máquina virtual de las que se realizó una copia de seguridad con protección de la aplicación.

Asegúrese de que habilita la protección de la aplicación cuando ejecuta la copia de seguridad primaria y cualquier copia de seguridad incremental subsecuente de la máquina virtual que alberga la aplicación de Microsoft SQL. Este método garantiza que las copias de las bases de datos de SQL de las que realizó una copia de seguridad de la máquina virtual se puede visualizar mediante Data Protection for SQL.

Bases de datos Microsoft SQL con nombres DBCS

Windows

Cuando tiene habilitado Data Protection for VMware para Unicode y puede realizar la copia de seguridad de las bases de datos de Microsoft SQL con nombres DBCS, Data Protection for SQL no está habilitado para Unicode. Por tanto, no puede utilizar Data Protection for SQL para restaurar las bases de datos con nombres DBCS desde una máquina virtual de la que se realizó una copia de seguridad con protección de la aplicación.

Para restaurar una copia de seguridad de máquina virtual que contiene las bases de datos de SQL con nombres DBCS, debe restaurar la copia de seguridad de máquina virtual completa de Data Protection for VMware.

Respuesta a mensajes de copias de seguridad de máquina virtual con protección de la aplicación

Windows

Puede que reciba algunos mensajes de aviso o de error durante las operaciones de copia de seguridad de máquina virtual cuando se utiliza la protección de la aplicación.

Es posible que se muestren los siguientes mensajes. Si es así, lleve a cabo las siguientes acciones:

ANS2196W An incompatible disk configuration is detected. Individual SQL Database Restore of database '<database_name>' is not supported.

Puede utilizar solo las bases de datos de Microsoft SQL que están en los discos básicos con la partición de Master Boot Record (MBR) para la recuperación de las bases de datos SQL individuales. Este mensaje identifica una o más bases de datos SQL que tengan una configuración de disco no compatible.

ANS2330E Failed to unfreeze the VSS writers because the snapshot time exceeded the 10 second timeout limitation.

Determine si hay un error llevando a cabo las siguientes acciones:

1. Utilice el cliente de vSphere para crear una instantánea de la máquina virtual inactiva. Si esta acción se realiza correctamente, pase al siguiente paso.

   Si esta acción no se realiza correctamente, es posible que el problema esté relacionado con VMware. Es posible que necesite ponerse en contacto con VMware Support y realice una consulta sobre el problema.
2. Realice una copia de seguridad de la máquina virtual sin protección de la aplicación:
   a. Inhabilite la protección de la aplicación eliminando la opción `INCLUDE.VMTSMVSS` *vmname* del archivo de opciones del cliente.
   b. Realice la copia de seguridad de la máquina virtual ejecutando el mandato siguiente desde la ventana Indicador de mandatos:

      ```
      dsmc backup vm vmname -vmbackuptype=fullvm
      ```

      Donde *vmname* es el nombre de la máquina virtual de la que desea realizar una copia de seguridad.

Los pasos que ha seguido hasta ahora pueden ayudarle a diagnosticar adicionalmente el problema y a solucionarlo. Sin embargo, si este paso no es satisfactorio, existe un problema con la máquina virtual invitada de Windows o con el cliente de archivado y copia de seguridad que hay en el nodo transportador de datos. Es posible que necesite la información de soporte para IBM Spectrum Protect que se encuentra en el IBM Support Portal para IBM Spectrum Protect.

Guardar los archivos de manifiesto VSS XML

Windows

Guardar los archivos de manifiesto VSS XML puede ayudarle a determinar qué bases de datos de Microsoft SQL se encuentran en la máquina virtual del invitado cuando se realiza la copia de seguridad.

Acerca de esta tarea

Los archivos de manifiesto VSS XML contienen información del grabador VSS que se genera durante una operación de copia de seguridad de máquina virtual. Archivos de manifiesto VSS XML necesarios para las operaciones de restauración VSS de las bases de datos seleccionadas de Microsoft SQL.

Procedimiento

Para guardar los archivos de manifiesto VSS XML en el nodo transportador de datos, siga estos pasos:

1. Añada la siguiente sentencia al archivo de opciones del cliente:

   ```
   testflag VMBACKup_SAVE_LOCAL
   ```

2. Inicie una copia de seguridad de la máquina virtual invitada con protección de la aplicación que alberga la aplicación SQL Server.

   Una vez finalizada la operación de copia de seguridad de máquina virtual completa, los archivos de manifiesto XML se guardan en la ubicación siguiente en el nodo de transportador de datos:

   ```
   C:\mnt\tsmvmbackup\fullvm\vmtsmvss\vm_name
   ```

   donde*vm_name* es el nombre de la máquina virtual de la que se ha realizado la copia de seguridad.

3. Ver la lista de bases de datos SQL que se encuentran en la máquina virtual invitada cuando se realiza la copia de seguridad al abrir el archivo`sqldbinfo.xml` con un editor de texto. Asegúrese de que el archivo `sqldbinfo.xml` contiene información completa sobre las bases de datos SQL de las que se realizó la copia de seguridad.

Determinar si una copia de seguridad de una máquina virtual puede fallar

Windows

Compruebe el estado de los grabadores VSS en una máquina virtual invitada para determinar si una copia de seguridad de una máquina virtual con protección de la aplicación podría fallar.

Acerca de esta tarea

Utilice el mandato **vssadmin list writers** para mostrar el estado de los grabadores VSS. Este mandato lista todos los grabadores que están disponibles en la máquina virtual de invitado, incluido el estado de los grabadores. Si uno o más de los grabadores VSS no están en un estado estable, la copia de seguridad de la máquina virtual con protección de la aplicación podría fallar.

Procedimiento

Desde la ventana Command Prompt, emita el siguiente mandato:

```
vssadmin list writers
```

El siguiente ejemplo muestra la salida del mandato:

```
Writer name: 'SqlServerWriter'
   Writer Id: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a}
   Writer Instance Id: {debc861a-7709-48b4-86a5-0a62457dc4a0}
   State: [1] Stable
   Last error: No error
```

El campo `State` indica el estado del grabador VSS.

Capítulo 3. Resolución de problemas del servidor de IBM Spectrum Protect

Al trabajar con el IBM Spectrum Protect, es posible que experimente problemas específicos del servidor. Las sugerencias para el diagnóstico del servidor que puede realizar van desde acciones simples, como reiniciar el servidor, hasta procedimientos más complejos.

La siguiente lista incluye algunas de las acciones que puede realizar para que le ayuden a resolver los problemas con el servidor.

- Reproducir el problema
- Comprobar el registro de actividad del servidor y otros registros
- Comprobar los registros de errores relacionados con la lectura o la grabación en un dispositivo
- Cambiar las opciones del servidor
- Detener e iniciar los servicios de planificación
- Consultar la base de datos o la agrupación de almacenamiento
- Rastrear la clase de rastreo UNICODE

Reproducción del problema

Reproduzca el problema para aislar la causa en una secuencia de sucesos concreta, si el problema se puede reproducir de forma rápida y coherente.

La mayoría de los problemas son el resultado de una combinación de eventos. Por ejemplo, la ejecución de la caducidad se produce junto con la realización de las copias de seguridad nocturnas planificadas correspondientes a 20 clientes. En algunos casos, el cambio del valor del tiempo o del orden de implementación de los eventos podría evitar que este problema volviera a producirse. Una forma de cambiar el valor del tiempo sería ejecutar la caducidad en un momento en el que no estén ejecutándose las copias de seguridad nocturnas planificadas de 20 clientes.

Comprobación del archivo de registro de actividad del servidor y de otros archivos de registro

Compruebe el archivo de anotaciones de actividad del servidor y busque los informes correspondientes a los 30 minutos previos y a los 30 minutos posteriores al momento de producirse el error.

Para revisar los mensajes de anotaciones de actividad del servidor, emita el mandato **QUERY ACTLOG**. Con frecuencia, otros mensajes pueden ofrecer información adicional acerca de la causa del problema y de la forma de solucionarlo.

Lista de archivos de registro adicionales

Es posible que el servicio de soporte de software de IBM le solicite que envíe los archivos de registro siguientes:

- Archivos de registro del servidor web:
  - `console.log`
  - `messages.log`
- Archivos FFDC (First-failure-data-capture):

- resumen_excepción_*fecha_hora*.log
- ffdc_*fecha_hora*.log

Ubicación de los archivos de registro

- Los archivos de registro del servidor web están en el siguiente directorio:

  AIX Linux *installation_dir*/ui/Liberty/usr/servers/guiServer/logs

  Windows *installation_dir*\ui\Liberty\usr\servers\guiServer\logs

  donde *installation_dir* es el directorio en el que está instalado IBM Spectrum Protect. Por ejemplo:

  AIX Linux /opt/tivoli/tsm

  Windows c:\Program Files\Tivoli\TSM
- Los archivos de registro FFDC están en la misma ubicación pero en el subdirectorio ffdc.

Comprobación de archivos de anotaciones de errores del sistema relativos a errores de dispositivo

Si el problema es un error que se ha creado al leer o grabar datos desde un dispositivo, la mayoría de los sistemas y dispositivos registran información en las anotaciones de errores del sistema.

Si un dispositivo o volumen que utiliza IBM Spectrum Protect notifica algún tipo de error en el registro de errores del sistema, es probable que se deba a un problema de dispositivo. Los mensajes de error registrados en las anotaciones de errores del sistema pueden proporcionar información suficiente para resolver el problema.

A continuación, se ofrecen algunos ejemplos de anotaciones de errores del sistema:

- errpt para AIX
- Anotaciones de eventos para Windows

Reversión de las opciones o de los valores del servidor

Si ha habido cambios de configuración en el servidor, intente volver a establecer los valores originales y realice de nuevo la operación que no ha podido ejecutarse correctamente.

Si la operación se ejecuta correctamente, intente aplicar los cambios de uno en uno y vuelva a intentar la operación hasta identificar el cambio de atributo que ha dado lugar al error.

Los cambios en el archivo de opciones de servidor, o de configuración del servidor, mediante los mandatos **SET** o **UPDATE** pueden producir anomalías para operaciones que se han ejecutado correctamente con anterioridad. La realización de cambios en el servidor para las clases de dispositivos, las agrupaciones de almacenamiento y las políticas también pueden causar errores en las operaciones que anteriormente se realizaron de forma correcta.

Reinicio del servicio de planificación

Las operaciones de cliente planificadas se ven afectadas por las definiciones de planificación en el servidor, así como el servicio de planificación (dsmsched) que se ejecuta en el propio sistema cliente.

Reinicie el servicio de planificación en el cliente si se produce un cambio en la planificación del servidor.

Importante: Si el servicio de planificación está gestionado por la aceptación de clientes, detenga y reinicie únicamente la aceptación de clientes.

Resolución de problemas de espacio en el servidor

La función principal del servidor de IBM Spectrum Protect es almacenar datos. Si no dispone de suficiente espacio en la base de datos o en las agrupaciones de almacenamiento, puede que las operaciones no se ejecuten correctamente.

Para determinar si la base de datos no dispone de espacio suficiente, emita el mandato **QUERY DB**. Si el porcentaje utilizado (espacio utilizado) es del 100%, o muy próximo a esta cifra, defina más espacio. Por lo general, si la base de datos no dispone de espacio suficiente, esta situación se indica mediante la emisión de otros mensajes del servidor.

Para determinar si una agrupación de almacenamiento no dispone de espacio suficiente, emita el mandato **QUERY STGPOOL**. Si el porcentaje utilizado es del 100%, o muy próximo a esta cifra, amplíe el espacio de almacenamiento disponible. Para añadir más espacio a la agrupación de almacenamiento DISK, asigne una o más agrupaciones de almacenamiento nuevas y defínalas para el servidor mediante el mandato **DEFINE VOLUME**. Puede configurar IBM Spectrum Protect para que asigne de forma automática espacio de agrupación de almacenamiento DISK y FILE utilizando el mandato **DEFINE SPACETRIGGER**.

Para añadir más espacio para una agrupación de almacenamiento de medios secuenciales, evalúe la biblioteca de cintas y determine si pueden añadirse más cintas reutilizables. En caso afirmativo, añada los volúmenes reutilizables adicionales a la biblioteca y actualice el parámetro **MAXSCR** para la agrupación de almacenamiento emitiendo el mandato **UPDATE STGPOOL**.

Asignación de memoria de servidor adicional

Si existen indicios de que su servidor no cuenta con recursos de memoria suficientes, asigne más memoria al mismo. Consulte la documentación del sistema operativo para obtener más información acerca de la adición de memoria.

Consejo: La cantidad de memoria que DB2 utiliza puede contribuir a informes que muestran que el sistema operativo ya no tiene memoria. Puede limitar la cantidad de memoria que DB2 utiliza incluyendo la opción `DBMEMPERCENT`. La opción `DBMEMPERCENT` especifica el porcentaje de espacio de dirección virtual que se dedica a los procesos del gestor de la base de datos.

Para asignar recursos de almacenamiento adicionales al servidor, complete las acciones siguientes:

- AIX Asegúrese de que haya espacio de paginación suficiente. También puede utilizar SMIT (System Management Interface Tool) para determinar si el número de aplicaciones causa escasez de memoria.
- Windows El método preferido de resolver una condición de memoria baja es añadir memoria física al sistema. De lo contrario, desde el panel de control, aumente la cantidad de almacenamiento virtual ejecutando el applet del sistema y aumentando el tamaño total del archivo de paginación.

Configuración de una instancia de servidor para utilizar la memoria compartida

Configure una instancia de servidor para utilizar la memoria compartida y ayudar a ralentizar las copias de seguridad de la base de datos que se puedan producir por los problemas de bucle de retorno del protocolo de control de transmisiones (TCP).

Acerca de esta tarea

En el siguiente procedimiento, debe actualizar la configuración del nodo de la base de datos para que el servidor pueda habilitar la memoria compartida.

- AIX Linux *server_bin_directory*/dbbkapi/dsm.sys
- Windows *server_instance_directory*\tsmdbmgr.opt

Procedimiento

1. Asegúrese de que el archivo de opciones del servidor, dsmserv.opt, contiene las siguientes líneas:

   ```
   COMMMethod SHAREdmem
   SHMPort         1510
   ```

2. AIX Linux Modifique la stanza para el nodo de copia de seguridad de la base de datos en el archivo de opciones de sistema de la API del cliente, dsm.sys.
   - Elimine las siguientes líneas de la stanza:

     ```
     COMMMethod TCPip
     TCPServeraddress 127.0.0.1
     TCPPort 1500
     ```

   - Añada las siguientes líneas a la stanza:

     ```
     COMMMethod SHAREdmem
     SHMPort 1510
     ```

3. Windows Modifique la stanza para la copia de seguridad de la base de datos en el archivo de opciones de sistema de la API del cliente, tsmdbmgr.opt.
   - Elimine las siguientes líneas del archivo tsmdbmgr.opt:

     ```
     COMMMethod TCPip
     TCPServeraddress 127.0.0.1
     TCPPort 1500
     ```

   - Añada las siguientes líneas al archivo tsmdbmgr.opt:

     ```
     COMMMethod SHAREdmem
     SHMPort 1510
     ```

Cambio de la frecuencia de copia

La política del servidor de IBM Spectrum Protect exige que el valor de la frecuencia de copia incremental no sea cero.

El atributo de frecuencia de copia de la clase de gestión *grupo_copia* actual para el archivo que se ha especificado dicta el número mínimo de días que deben transcurrir entre copias de seguridad incrementales sucesivas. Si tiene la intención de realizar una copia de seguridad incremental en un archivo y se establece un número superior a 0 días, el archivo no se enviará al servidor, aunque haya cambiado.

Se pueden completar una serie de pasos para corregir este problema:

- Póngase en contacto con el administrador del servidor para cambiar el atributo de frecuencia de copia.
- Emita una copia de seguridad selectiva del archivo. Por ejemplo, `DSMC SELECTIVE C:\FILE.TXT`

Puede emitir el mandato **QUERY COPYGROUP** para determinar el valor del parámetro de frecuencia de copia:

```
tsm: WINBETA>q copygroup standard active f=d
Nombre dominio políticas: STANDARD
 ...
Copy Frequency: 1
 ...
```

Resolución de errores de operaciones de RELABEL

Si ejecuta una operación RELABEL cuando todas las unidades están ocupadas, el volumen de destino no podrá volverse a etiquetar porque no puede obtener una unidad. Las unidades ocupadas son unidades que están en uso para operaciones normales como la copia de seguridad, la restauración, la migración y la reclamación.

Cuando se produce un error de RELABEL, se crea la siguiente información de ejemplo:

```
ANR0984I Process 25 for RELABEL started in the BACKGROUND at 22:10:36.
ANR8799I RELABEL: Operation for library IBMVTL started as process 25.
ANR1341I Scratch volume 007403 has been deleted from storage pool VTLPOOL.
ANR8847E No LTO-type drives are currently available in library IBMVTL.
ANR8801I LABEL LIBVOLUME process 25 for library IBMVTL completed; 0 volume(s)
labeled, 0 volume(s) checked-in.
ANR0985I Process 25 for RELABEL running in the BACKGROUND completed with
completion state SUCCESS at 22:10:36.
```

Para resolver un error RELABEL, siga estos pasos:

1. Asegúrese de que se deja disponible una unidad para la operación RELABEL y vuelva a etiquetar un volumen de destino.
2. Actualice las clases de dispositivos que apuntan a la biblioteca. Actualice las clases de dispositivos con un valor de parámetro **MOUNTLIMIT** que sea inferior al número total de unidades disponibles.

   Si una operación RELABEL no puede obtener una unidad o falla en volver a etiquetar un volumen, IBM Spectrum Protect intentará volver a etiquetar el volumen durante cada operación futura de RELABEL.

Si la operación RELABEL falla, emita el mandato **LABEL LIBVOLUME** para todos los volúmenes que se han dado de baja de IBM Spectrum Protect pero que no se han vuelto a etiquetar. Incluya los siguientes parámetros con el mandato **LABEL LIBVOLUME**:

```
SEARCH=YES LABELSOURCE=BARCODE OVERWRITE=YES CHECKIN=SCRATCH
```

Evitar errores de comunicación durante el proceso de importación

Los errores de comunicación se muestran en el registro de actividad del servidor de destino si cancela el proceso de importación desde el servidor de destino.

Si cancela el proceso de importación desde el servidor de destino, los mensajes de error de comunicación del registro de actividad muestran el nombre de nodo que inició la operación de exportación desde el servidor de origen. Por ejemplo, los siguientes mensajes se pueden mostrar en el registro de actividad del servidor:

```
ANR0440W Protocol error on session 2 for node ADMIN
ANR3174E Communication error with managed server ADMIN.
ANR0484W Session 2 for node ADMIN terminated - protocol violation detected.
```

Puede ignorar los mensajes de error de comunicación en el registro de actividad del servidor de destino al que pertenece el proceso de importación. De forma alternativa, si cancela el proceso de importación desde el servidor de origen, no se produce ningún mensaje de error en el servidor de origen ni en el de destino.

Adición de un certificado autofirmado al almacén de claves

Puede configurar comunicaciones seguras mediante un certificado autofirmado con el sistema de almacenamiento de objetos. En esta situación, IBM Spectrum Protect utiliza `HTTPS` en lugar de `HTTP` cuando se comunica con el sistema de almacenamiento de objetos. Los siguientes pasos constituyen un método para importar certificados.

Acerca de esta tarea

Utilice un navegador web para obtener una copia del certificado que utiliza el sistema de almacenamiento de objetos. Los siguientes pasos son específicos de Firefox, pero otros navegadores proporcionan funciones similares. Consulte las instrucciones de su navegador preferido sobre cómo exportar certificados.

Procedimiento

1. Obtenga el certificado que utiliza el servidor OpenStack Swift o IBM Cloud Object Storage.
   a. Escriba el URL correspondiente al sistema de almacenamiento de objetos en la barra de direcciones del navegador y pulse **Intro**. Utilice el URL del servidor clave para OpenStack o el URL del nodo de la aplicación de acceso para IBM Cloud Object Storage.

      Sugerencia: si utiliza IBM Cloud Object Storage como sistema de almacenamiento de objetos, inicie la sesión en IBM Cloud Object Storage y pulse el separador **Seguridad**. En la sección **Huella digital dsNet**, pulse **entidad emisora de certificados dsNet** y copie la información del certificado en un archivo de certificado para el componente 2.
   b. Acepte los avisos que muestre el navegador.
   c. Pulse el icono de bloqueo en la barra de direcciones del navegador.
   d. Seleccione **Más información** en la ventana emergente.

e. Seleccione **Ver certificado** en la ventana Información de página.
f. Pulse el separador **Detalles** en la página Visor de certificados y, a continuación, seleccione **Exportar**.
g. Guarde el archivo exportado en la ubicación que desee.

2. Añada el certificado al almacén de claves predeterminado de Java.

   En los siguientes pasos, se presupone que los nodos de cliente están en Linux y que el servidor se está ejecutando en Linux. Puesto que cada persona que accede a IBM Cloud Object Storage tiene su propio certificado de forma predeterminada, añada el certificado correspondiente a cada uno al almacén de claves y utilice un alias diferente para cada certificado.

   a. Abra un terminal y vaya al directorio `jre/bin`.

      La ubicación de instalación predeterminada es `/opt/tivoli/tsm/jre/bin`.

   b. Realice una copia de seguridad del archivo `cacerts` de Java ejecutando el siguiente mandato: `cp ../lib/security/cacerts ../lib/security/cacerts.original`.

      En un sistema Windows, la ubicación del almacén de claves `cacerts` de Java es: *`dir_instalación`*`\jre\lib\security\` y la ubicación de la herramienta de claves es *`dir_instalación`*`\jre\bin\`.

   c. Importe el certificado guardado en el procedimiento anterior ejecutando el siguiente mandato: `./keytool -import -keystore ../lib/security/cacerts -alias` *`somealias`* `-file` *`yourfile`*

      donde *`somealias`* es un alias exclusivo para este certificado en el almacén de claves, lo que resulta importante si tiene más de un certificado, y *`yourfile`* es la vía de acceso y nombre de archivo del certificado del primer paso de estas instrucciones.

   d. Cuando se le solicite la contraseña, escriba *changeit*. Si ha cambiado la contraseña predeterminada, escriba su contraseña actual.

   e. Cuando se le pregunte si es un certificado fiable, escriba *yes*.

      Cuando el certificado se añade correctamente, se muestra el siguiente mensaje: `El certificado se ha añadido al almacén de claves`. Los certificados predeterminados caducan en poco tiempo. Cuando caducan, puede perder el acceso al almacén de objetos hasta que actualice los certificados. Puede crear sus propios certificados y utilizarlos, aunque la creación e instalación de estos certificados en sistemas de almacenamiento de objetos queda fuera del ámbito de este documento.

   f. Reinicie el servidor de IBM Spectrum Protect.

Determinación del motivo por el que faltan los registros de un suceso de copia de seguridad del cliente

Si una sesión de comunicaciones de cliente/servidor finaliza de forma anómala, es posible que se produzca un retardo antes de que los registros de resumen de un suceso de copia de seguridad del cliente se añadan a la base de datos del servidor.

Síntoma

Una vez completado el proceso de copia de seguridad de un cliente, el registro no se añade a la base de datos inmediatamente. El registro de resumen puede tardar varias horas en añadirse a la base de datos.

Causas

Los registros de resumen pueden tardar varias horas en añadirse a la base de datos del servidor debido a que una sesión del servidor debe esperar a que se complete el proceso de finalización anómala. Una sesión puede finalizar de forma anómala por los motivos siguientes:

- Errores de red
- Tiempos de espera de sesión excedidos

Se pueden exceder los tiempos de espera cuando los procesos de copia de seguridad tardan más de lo previsto.

Resolución del problema

1. Para determinar por qué las sesiones de comunicación entre cliente y servidor finalizan de forma anómala, realice las acciones siguientes:
   a. Revise el registro de actividad emitiendo el mandato **QUERY ACTLOG**.
   b. Revise el registro de errores del cliente, `dsmerror.log`, en el directorio de instalación del cliente.
   c. Si no puede determinar la causa del problema revisando la actividad del registro, habilite el rastreo para el cliente de copia de seguridad/archivado.
2. Resuelva los problemas de comunicación. Puede trabajar con el equipo de red para recopilar y analizar los datos de red.

Referencia relacionada:

"Habilitación del rastreo de cliente de archivado y copia de seguridad" en la página 165

Resolución de la instalación y problemas de actualización

La resolución de los problemas de instalación con el servidor de IBM Spectrum Protect puede implicar la revisión de archivos de anotaciones, la reinstalación del servidor o muchas otras posibles opciones.

Archivos de registro de instalación

Si se producen errores durante el proceso de instalación, estos errores se registran en archivos de registro.

Para ver los archivos de registro de instalación, haga clic en **Archivo** > **Ver registro** en la herramienta de gestión de la instalación. Para recopilar estos archivos de registro, pulse en**Help** > **Export Data for Problem Analysis** en la herramienta de gestión de la instalación.

Los archivos de registro están almacenados en el directorio de registros de IBM Installation Manager:

AIX Linux `/var/ibm/InstallationManager/logs`

Windows `C:\ProgramData\IBM\Installation Manager\logs`

El asistente de instalación falla al iniciarse

El IBM Installation Manager requiere las biblioteca GTK para dar soporte a la interfaz gráfica de usuario (GUI) en sistemas AIX. Si estas bibliotecas no están instaladas antes de instalar el servidor IBM Spectrum Protect, la instalación no podría empezar. Se emite un error sobre las bibliotecas GTK.

Información relacionada:

Instalación de IBM Spectrum Protect mediante el asistente de instalación

Resolución de los problemas de instalación de GSKit

Al utilizar el software de instalación de IBM Spectrum Protect , se instala automáticamente la versión correcta de Global Security Kit (GSKit).

Si el entorno de instancias del servidor IBM Spectrum Protect no está configurado correctamente, puede que el servidor no cargue las bibliotecas GSKit adecuadas. El asistente de configuración de instancias del servidor le ayuda a evitar muchos problemas que pueden ser frecuentes cuando se configura manualmente la instancia.

Windows Emita el siguiente mandato:

```
set PATH=X:\Program Files\IBM\gsk8\bin;X:\Program Files\IBM\gsk8\lib64;%PATH%
```

donde *X* es la unidad del sistema. La variable de entorno PATH se modifica para apuntar al directorio correcto.

Linux Actualice la `LD_LIBRARY_PATH` o shell emitiendo el siguiente comando:

```
export LD_LIBRARY_PATH=platform-specific-gskit-library-directory:$LD_LIBRARY_PATH
```

donde *platform-specific-gskit-library-directory* es uno de estos directorios, según su plataforma:

- Linux `/usr/local/ibm/gsk8_64/lib64`

AIX Para AIX, emita el siguiente comando:

```
export LIBPATH=/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

AIX Linux Debe actualizar los siguientes archivos para establecer la vía de acceso a bibliotecas cuando el servidor DB2 o el servidor se ha iniciado:

- *directorio_instancia*`/sqllib/usercshrc`
- *directorio_instancia*`/sqllib/userprofile`

En el archivo *directorio_instancia*`/sqllib/usercshrc`, añada estas líneas:

- AIX

  ```
  setenv LIBPATH /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
  ```

- Linux

  ```
  setenv LD_LIBRARY_PATH /usr/local/ibm/gsk8_64/lib64:$LD_LIBRARY_PATH
  ```

En el archivo *directorio_instancia*`/sqllib/userprofile`, añada estas líneas:

- AIX

  ```
  LIBPATH=/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
  export LIBPATH
  ```

- Linux

```
LD_LIBRARY_PATH=/usr/local/ibm/gsk8_64/lib64:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH
```

Verifique la configuración de vía de acceso a biblioteca y a la versión GSKit emitiendo los siguientes comandos:

- AIX

```
echo $LIBPATH
gsk8capicmd_64 -version
```

- Linux

```
echo $LD_LIBRARY_PATH
gsk8ver_64
```

Si la versión de GSKit no es 8.0.14.28 o posterior, debe volver a instalar el servidor. La reinstalación garantiza que la versión de GSKit correcta está disponible.

No se han creado instancias para el servidor durante la actualización

Cuando una conexión no se pueda establecer, el instalador no puede recrear las instancias del servidor de IBM Spectrum Protect. Debe recrear manualmente las instancias del servidor.

Acerca de esta tarea

El asistente de instalación utiliza los métodos siguientes para establecer una conexión con el sistema para recrear las instancias del servidor:

- AIX Linux Secure shell (SSH)
- Windows Bloque de mensajes de servidor (SMB) de Windows

Cuando utilice uno de estos métodos en el puerto predeterminado, el puerto no se puede bloquear mediante un cortafuegos. Si se bloquea, siga estos pasos para actualizar manualmente la instancia del servidor. AIX Linux

Procedimiento

1. Cierre el asistente de instalación.
2. Siga los pasos siguientes para cada instancia del servidor:
   a. Cuando la actualización haya finalizado, emita el mandato siguiente para recrear la instancia:

      ```
      /opt/tivoli/tsm/db2/instance/db2icrt –u usuario_instancia nombre_instancia
      ```

   b. Recree las variables en el archivo de instancias. Emita el mandato **db2set -i** para cada variable del archivo de instancias. Por ejemplo, establezca la variable *DB2COMM* para que sólo sea TCPIP para la instancia MYINST:

      ```
      /opt/tivoli/tsm/db2/instance/db2set –i MYINST DB2COMM=TCPIP
      ```

      Para mostrar una lista de todas las variables definidas, especifique el parámetro **-all**; por ejemplo, **db2set -all**.
   c. Emita el mandato **db2stop** para detener la instancia de base de datos.
   d. Utilice el ID de usuario que tiene la instancia del servidor para emitir el mandato **db2start** para iniciar la instancia de base de datos.
   e. Catalogue y actualice cada base de datos emitiendo los mandatos siguientes:

      ```
      db2 catalog db TSMDB1 on "vía_de_acceso_base_datos"
      db2 upgrade db TSMDB1
      ```

f. Emita el mandato **db2stop**.
g. Inicie el servidor.

Resolución de una situación de proceso de desinstalación detenido

La caducidad de una contraseña de usuario de una instancia de DB2 puede provocar que el proceso de desinstalación de IBM Spectrum Protect se detenga antes de completarse.

Si la contraseña del ID de usuario de la instancia de DB2 ha caducado, el proceso de desinstalación no se puede completar. Debe iniciar sesión mediante la utilización del ID de instancia de DB2 y reiniciar la contraseña, después desinstalar IBM Spectrum Protect.

El despliegue automático del cliente no ha actualizado el software del cliente

Si la planificación del despliegue se completa pero el software de cliente no se actualiza al nivel de destino,revise los archivos de registro en el sistema del cliente.

Síntoma

El software del cliente no se ha actualizado al nivel de destino después de completarse el despliegue automático.

Causa

Los siguientes ejemplos son algunas de las razones por las cuales el software del cliente no se actualiza al nivel de destino.

- No hay espacio suficiente disponible en el sistema de archivos del cliente para completar la actualización.
- Los problemas de red han impedido que los datos se transfieran del servidor al sistema del cliente.

Resolución del problema

Puede resolver el error de actualización del cliente si revisa el registro y los archivos de rastreo en el sistema del cliente. El gestor de despliegue escribe los datos de registro y de rastreo para una operación de despliegue al sistema de archivos del cliente. La ubicación para los archivos de registro se especifica en la definición de la planificación del despliegue en el servidor.

Complete los siguientes pasos para resolver el error de actualización del cliente:

1. Cambie los directorio a la ubicación de los archivos de registro.
   - AIX La ubicación predeterminada es`/usr/tivoli/client/IBM_ANR_UNX/Vxxxx/log`.
   - Linux La ubicación predeterminada es`/opt/tivoli/tsm/client/IBM_ANR_UNX/Vxxxx/log`.
   - Mac OS X La ubicación predeterminada es `/Library/Application Support/tivoli/tsm/client/ba/bin/IBM_ANR_MAC/Vxxxx/log`.
   - Windows La ubicación predeterminada es `C:\Program Files\Tivoli\TSM\IBM_ANR_WIN\Vxxxx\log`.

Donde el directorioV*xxxx* de la vía representa el nivel de destino del cliente de archivado y copia de seguridad.

2. Revise los archivos de registro y de rastreo desde el gestor de despliegue para determinar la causa principal del fallo de actualización del cliente. Tabla 5 muestra una lista de archivos de registro que puede revisar.

Tabla 5. Descripción de los archivos de registro

Nombre del registro	Descripción
`setup.log`	Registro de errores que muestra mensajes de error, avisos e información.
`trace.txt`	El rastreo del cliente muestra información detallada sobre los procesos de actualización del cliente.
`updatemgr.log`	Registro del gestor de despliegue que muestra información sobre los procesos de despliegue.

Resolución de detenciones del servidor

Las detenciones del servidor se pueden producir desde errores de proceso, el manejador de condición de excepción del sistema, u otros errores. Cuando determine el origen de la detención del servidor, el motivo puede resolver otros problemas conocidos.

La detención del servidor puede deberse a uno de los siguientes motivos:

- Un error de proceso da lugar a una sobregrabación de la memoria o algún otro evento desencadena el manejador de condición de excepción del sistema para finalizar el proceso del servidor.
- El proceso del servidor tiene algoritmos de validación en la aplicación que comprueban diversas condiciones antes de continuar con la ejecución. Como parte de esta comprobación de validación, existen casos en los que, si la comprobación de validación no es correcta, el servidor se encargará de llevar a cabo su propia finalización en lugar de permitir que continúe el proceso. Estas validaciones de catástrofes se denominan aserciones o asertos. Si el servidor finaliza debido a una aserción, se emite el mensaje siguiente:

  `ANR7837S Se ha detectado el error interno XXXNNN.`

  donde *XXXNNN* es un identificador que se ha asignado al error de aserción.

Otros mensajes del servidor que indican que se ha detenido el sistema son ANR7836S y ANR7838S.

Si el servidor se ha detenido como resultado de una aserción o de un manejador de condición de excepción del sistema, el programa de utilidad tsmdiag puede recopilar la siguiente información y empaquetarla para enviarla al servicio de IBM para que pueda diagnosticarse la situación:

- Archivo de errores del servidor (`dsmserv.err`)
- Imagen del sistema (archivo de núcleo)
- Bibliotecas y otros archivos
- Anotaciones del sistema
- Anotaciones de actividades

Empaquete todos los (archivos) de datos recopilados y póngase en contacto con el servicio de IBM para notificar este problema.

Tareas relacionadas:

Apéndice B, “Ejecute el programa de utilidad tsmdiag”, en la página 217

Resolución de un problema de detención o bucle

Una detención es una situación en la que un servidor no se inicia o no completa una función o no utiliza toda la potencia de los microprocesadores.

Una detención puede consistir únicamente en una sesión o un proceso que no se está procesando, o bien puede tratarse de todo el servidor de IBM Spectrum Protect que no responde. Un bucle hace referencia a aquellas situaciones en las no hay ningún progreso, pero el servidor sigue utilizando una gran cantidad de potencia de los microprocesadores. Un bucle puede afectar únicamente a una sesión o proceso, o bien puede afectar a todo el servidor.

Puede recopilar información para solucionar este tipo de problema, en función de si el servidor puede o no responder a los mandatos. Hay disponible un Script Perl para recopilar datos del servidor. Es recomendable planificar la lista de mandatos **SHOW** para que se ejecute de forma intermitente y pueda ver el comportamiento que precede a la situación de detención.

- Cuando se haya producido una situación de detención o un bucle en la que el servidor puede responder a los mandatos, emita los siguientes mandatos como ayuda para determinar la causa que ha dado lugar a que el proceso dejara de responder:
  - **QUERY SESSION f=d**
  - **QUERY PROCESS**
  - **SHOW RESQ**
  - **SHOW THREADS**
  - **SHOW DEADLOCK**
  - **SHOW TXNT**
  - **SHOW DBTXNT**
  - **SHOW LOCKS**
  - **SHOW LIBR**
  - **SHOW MP**
  - **SHOW SESS**
  - **SHOW ASQ**
  - **SHOW ASVOL**
  - **SHOW DBV**
  - **SHOW SSS**
  - **SHOW CSV** (Emita este mandato solo cuando el problema esté relacionado con la planificación.)
- Cuando un servidor se cuelga o se crean bucles, emita los siguientes mandatos para proporcionar una instantánea de diagnóstico detallada del entorno de IBM Spectrum Protect:

  ```
  db2fodc -hang -alldbs
  db2support . -d base_de_datos -s
  ```

  Puede utilizar el archivo `db2support.zip` que se generó para la resolución de problemas.

- Además de la salida de los mandatos que se indican, o en caso de que el servidor no pueda responder a los mandatos, recopile un vuelco. La forma de recopilar un vuelco dependerá del sistema operativo utilizado.
  - AIX Linux Emita el comando **KILL -11** en el proceso dsmserv para crear un archivo principal. Para ejecutar el mandato "kill", obtenga la ID del proceso emitiendo el mandato **PS**.
  - Windows Realice una búsqueda para recopilar volcados de modalidad de usuario en el sitio web de Microsoft en http://support.microsoft.com/.

Resolución de problemas de estado de espera con servidores de repositorio de usuario externo

Si parece que el servidor de IBM Spectrum Protect no responde, es posible que esté relacionado con el sistema operativo y el uso del sistema operativo de un repositorio de usuario externo.

Antes de empezar

El rendimiento lento del servidor se puede atribuir a que un sistema operativo que utiliza un repositorio de usuario externo tiene definidos demasiados grupos de usuarios. Los servidores NIS (Network Information Service) y LDAP (Lightweight Directory Access Protocol) son dos tipos de servidores de repositorio de usuario externo.

Un ejemplo de comportamiento que no responde se produce cuando IBM Spectrum Protect tarda mucho tiempo en conectarse al servidor de IBM DB2 . Otro ejemplo es cuando parece que el servidor no responde a las solicitudes administrativas.

Acerca de esta tarea

Complete los siguientes pasos para resolver un problema de estado de espera que ocurre con los siguientes servidores cuando utiliza un servidorde LDAP:

Procedimiento

1. Detenga el servidor de IBM Spectrum Protect.
2. AIX Emita los mandatos siguientes:
   a. `db2set DB2_ALTERNATE_GROUP_LOOKUP=GETGRSET`
   b. `db2stop force`
   c. `db2start`

   Linux Emita los mandatos siguientes:
   a. `db2set DB2_ALTERNATE_GROUP_LOOKUP=GETGROUPLIST`
   b. `db2stop force`
   c. `db2start`
3. Reinicie el servidor.

Búsqueda del archivo de error del servidor(dsmserv.err)

Cuando el servidor se detiene, éste añade información al archivo dsmserv.err que se encuentra en el mismo directorio que el servidor.

Antes de empezar

AIX Linux El manejador de rupturas está inhabilitado para impedir que el rastreo inverso de función se imprime en la consola y en el archivo dsmserv.err . Este es un cambio que debe aplicarse para garantizar la obtención de un archivo de núcleo lo más completo posible. Como parte de la inhabilitación del manejador de condición de excepción, se encuentra un nuevo script, getcoreinfo en los paquetes de Linux. El script getcoreinfo obtiene la función de rastreo regresivo para la hebra anómala y registra valores y la función de rastreo regresivo para todas las demás hebras. La cantidad de información disponible en el núcleo para otras hebras sigue incompleta en algunas plataformas/distribuciones de Linux. Consulte el script getcoreinfo (en el directorio bin del servidor) para obtener más detalles.

Windows Si el servidor se está ejecutando como un servicio, el archivo se denomina dsmsvc.err.

Acerca de esta tarea

Siga estos pasos para capturar el archivo de errores del servidor:

Procedimiento

1. Asegúrese de que el depurador GNU (gdb) se ha instalado en el sistema cliente.
2. Copie el script de shell gt al directorio bin del servidor (donde se encuentran el archivo ejecutable del servidor [.exe] y el archivo de núcleo).
3. Asegúrese de que el script sea un archivo ejecutable (chmod a+x gt).
4. Invoque el script con las vías de acceso/nombres del archivo ejecutable (el valor predeterminado es ./dsmserv) y del núcleo (el valor predeterminado es ./dsmcore). La salida está en el archivo dsm_gdb.info (que debería enviarse a IBM).

Búsqueda de la imagen del sistema (archivo de núcleo)

Por lo general, un archivo de núcleo u otra imagen del sistema de la memoria es utilizada por IBM Spectrum Protect durante la anomalía.

En cada caso, redenomine el archivo de núcleo para impedir que una posterior interrupción del sistema sobrescriba el archivo. Por ejemplo, el nombre de un archivo debería cambiarse por “core.Aug29” en lugar de “core.” El tipo y el nombre del archivo de núcleo varían en función de la plataforma.

- AIX Linux Generalmente se crea un archivo denominado core. Asegúrese de que existe suficiente espacio en el directorio del servidor para que pueda tener lugar una operación de volcado. Es habitual tener un archivo de volcado de 2 GB para el servidor de IBM Spectrum Protect de 32 bits. Asimismo, asegúrese de que el valor ulimit de los archivos de núcleo se ha establecido en "unlimited" para evitar que se trunque el archivo de vuelco.
- Windows El contenido del sistema se vuelva automáticamente a través de una llamada de interfaz de programación de aplicaciones del sistema (API). Si el

servidor se ejecuta como servicio, el archivo de vuelco se denomina `dsmsvc.dmp`. De lo contrario, el archivo de volcado se llamará `dsmserv.dmp`

Si el sistema no se ha configurado para capturar un archivo de núcleo o el sistema no disponía de suficiente espacio para crear un archivo de núcleo completo, puede que su utilidad para determinar la causa del problema sea limitada.

Recuperación de archivos de biblioteca para el análisis del núcleo

AIX Linux

Los archivos principales son específicos para la aplicación, bibliotecas y otros recursos del sistema en uso por la aplicación en el sistema donde se estaba ejecutando.

Para leer debidamente el archivo de núcleo en el sistema, se necesitan todos los archivos que se indican a continuación, que se encuentran en el directorio en el que está instalado el servidor:

- `dsmserv`
- `dsmlicense`
- `ndmpspi`
- `dsmcored`
- `dsmaio`
- `centera`

Los archivos de biblioteca necesarios varían en función de la plataforma:

- AIX Recopile los siguientes archivos:
  - `/usr/ccs/lib/libpthreads.a`
  - `/usr/ccs/lib/libc.a`
  - Recopile cualquier otra biblioteca cargada, como las salidas de mensajes. Para ver las bibliotecas que están cargadas, invoque dbx emitiendo el comando **dbx dsmserv core_file** . A continuación, desde la solicitud dbx, emita el comando **map** para mostrar todas las bibliotecas que se cargan y que son necesarias para el análisis principal.
- Linux Emita el comando **ldd dsmserv** y envíe todas las bibliotecas dinámicas compartidas. Por ejemplo:
  - `libm.so.6 =>/lib64/libm.so.6`
  - `libnsl.so.1 =>/lib64/libnsl.so.1`
  - `libpthread.so.0 =>/lib64/libpthread.so.0`
  - `libdl.so.2 =>/lib64/libdl.so.2`
  - `libc.so.6 =>/lib64/libc.so.6`
  - `/lib64/ld64.so.1 =>/lib64/ld64.so.1`

Recuperación de archivos de registro del sistema

Puede recuperar los archivos de registro del sistema para ayudar a resolver las causas de las detenciones del servidor.

Recupere los siguientes archivos de registro para proporcionárselos al servicio de IBM:

- AIX Redirija la salida del mandato **errpt -a** a un archivo: `errpt -a >errpt.txt`.
- Linux Copie el archivo `/var/log/messages`.
- Windows Guarde una copia de los Registros de sucesos, como se muestra en el visor de sucesos.

Recuperación del registro de actividades

Puede recuperar archivos de registro de actividades para que le ayuden a resolver problemas de detenciones del servidor.

Vea y recopile las entradas del registro de actividades que comienzan al menos dos horas antes de la detención y 30 minutos después de que se produjera emitiendo el mandato **QUERY ACTLOG**.

Detección de errores una vez que se inicie y se detenga un servicio del servidor

Windows

Si un servicio del servidor se inicia y se detiene de forma inesperada, puede determinar la causa del error solicitando un archivo de anotaciones de errores.

Acerca de esta tarea

Se puede iniciar un servicio desde la aplicación de Windows Services. Una vez que inicie el servicio, el servicio puede indicar que se ha iniciado, pero tras reiniciarse, el servicio indicará que se ha detenido. En los pasos siguientes, "Server1" se utiliza como el nombre del servidor que se inicia y se detiene. Para determinar la causa del error para Server1, finalice los pasos siguientes:

Procedimiento

1. Amplíe **Tivoli Storage Manager** > **[*Nombre_host*] (Windows - Local)** > **Server1** > **Informes** > **Información de servicio** para mostrar el servicio del servidor.
2. En el panel de la derecha, pulse el botón derecho sobre el servicio de **Server1** y seleccione **Propiedades**.
3. Seleccione la opción **Anotar salida en archivo** y pulse **Aceptar**.
4. Inicie el servicio Server1.
5. Si el servicio se detiene de nuevo, abra un editor de texto para leer el contenido del siguiente archivo:

   `C:\Archivos de programa\Tivoli\TSM\Server1\console.log`
6. Determine la causa del error revisando los mensajes de error que se generan.

El directorio sqllib/db2dump provoca la conclusión

Los servidores Tivoli Storage Manager V6 pueden concluir de forma inesperada si el directorio `sqllib/db2dump` se sobrecarga. La hora más común para una conclusión es cuando los archivos FODC (first occurrence data capture) de DB2 se graban en el directorio.

El directorio `sqllib/db2dump` es una vía de acceso de directorio de datos de diagnóstico que DB2 utiliza para grabar información diagnóstica para FODC. En el tiempo, DB2 puede grabar muchos archivos FODC en el directorio relacionados con el estado de la base de datos. Cuando los archivos no se eliminan ni se suprimen, el sistema de archivos puede quedar lleno. La ubicación de los archivos FODC (first occurrence data capture) de DB2 depende de los valores de configuración de DB2 o de los valores de la variable ambiental de DB2.

Ubique el directorio de información de diagnóstico marcando los valores de configuración de DB2 o los valores de variables ambientales de DB2. Si los archivos de la vía de acceso del directorio de diagnóstico hacen que el sistema de archivos se llene, realice una de las siguientes acciones:

- Agregue espacio al sistema de archivos.
- Mueva los archivos a otro sistema de archivos. Consulte Tabla 6.
- Utilice el servidor para archivar los archivos y, a continuación, suprímalos utilizando los pasos siguientes:
  1. Ejecute el programa de utilidad db2support para recopilar la información de diagnóstico del sistema de DB2.
  2. Archive los archivos de diagnóstico y el archivo `db2support.zip` que se listan en Tabla 6 en el servidor con el cliente.
  3. Suprima los archivos que se listan en Tabla 6.

Tabla 6. Archivos que se pueden suprimir una vez archivados

Nombre de archivo	Descripción
`instance_name.nfy` `instance_name.`*`n`*`.nfy` (donde *n* es un número)	Registros de notificaciones de administración
`db2dasdiag.log`	Registro de diagnóstico de servidor de administración de DB2 (DAS)
`db2eventlog.`*`xxx`* (donde *xxx* es el número de partición de la base de datos)	Registro de eventos de DB2
`nnnnnnn.nnnnn.nnn``.dump.bin` (donde *n* es un número)	Archivos de volcado binarios de estructuras en memoria claves
`nnnnnnn.n.nnn``.trap.txt` (donde *n* es un número)	Archivo de interrupción
`nnnnnnn.nnnnn.nnn``.apm.bin` (donde *n* es un número)	Acceder a los archivos de volcado binarios del gestor de planificación
`nnnnnnn.nnnnn.nnn``.stack.txt` (donde *n* es un número)	Seguimientos de la pila

Tabla 6. Archivos que se pueden suprimir una vez archivados (continuación)

Nombre de archivo	Descripción
FODC_*xxxx*/core<pid>	Archivos principales Estos directorios FODC_*xxx* contienen la indicación de fecha y hora en el nombre del directorio. Guarde los directorios más recientes y sus archivos. El historial puede ser útil para posibles problemas de diagnóstico futuros relacionados con la base de datos. Se guardará una directriz al menos una semana.
events/db2optstats.*n*.log (donde *n* es un número)	Archivo de registro de estadísticas

Consejo: No suprima el archivo db2diag.log ni los archivos dentro del directorio stmmlog. El historial que contienen puede ser útil para diagnosticar problemas del servidor relacionados con la base de datos.

Referencia relacionada:

"Ubicación de los archivos de registro de diagnóstico de DB2" en la página 79

Resolución de problemas con la verificación de páginas de base de datos

Un error en la validación de páginas durante el proceso de copia de seguridad de base de datos puede indicar que la base de datos está dañada y requiere una acción de reparación para corregir el problema. Si falla la validación de páginas, la copia de seguridad de base de datos también falla.

Procedimiento

- Póngase en contacto con el servicio de soporte de IBM para obtener ayuda acerca de cómo diagnosticar y reparar los daños en la base de datos.
- Si estaba en proceso una copia de seguridad de base de datos para liberar espacio en el directorio del registro de archivado, realice una de las acciones siguientes:
  - Aumente la cantidad de espacio en el directorio de registro de archivado.
  - Emita la opción ARCHFAILOVERLOGDIRECTORY para especificar un directorio de registro de archivado de migración tras error en el que el servidor pueda almacenar los archivos de registro que no puede almacenar en el directorio de registro de archivado.

  Asegurarse de que el espacio del directorio de registro de archivado es el adecuado permite que el servidor continúe ejecutándose mientras se reparar la base de datos.

Resolución de errores de bases de datos

Los errores de base de datos pueden causarse por problemas como la falta de espacio o por errores producidos por operaciones de inserción, actualización o supresión.

Los usuarios que sean administradores experimentados de DB2 puede ejecutar consultas de SQL avanzadas y utilizar herramientas de DB2 para supervisar la base de datos, el espacio que se está utilizando y cualquier error. Cuando ejecute estas consultas, no utilice las herramientas de DB2 para cambiar los ajustes de configuración de DB2 de los ajustes predefinidos mediante IBM Spectrum Protect o, no utilice ningún otro software para modificar estos ajustes. El servidor debe utilizarse con el idioma de definición de datos y la configuración de base de datos que despliega IBM Spectrum Protect.

Para obtener más información, consulte la Información sobre el producto DB2.

Resolución de problemas de inicio del gestor de base de datos

Es posible que el servidor de IBM Spectrum Protect no se inicie si el gestor de base de datos de DB2 está configurado para utilizar el complemento de `dsmdb2pw`. Cuando el servidor no pueda cargar el complemento, el gestor de la base de datos no se iniciará y, a su vez, el servidor no se iniciará.

Debido al problema del complemento, el servidor emite un mensaje de error similar a este ejemplo:

```
db2start
SQL1365N  db2start or db2stop failed in processing the plugin "dsmdb2pw".
Reason code = "10".
04/26/2011 16:04:11     0   0   SQL1365N
db2start or db2stop failed in processing the plugin "". Reason code = "".
```

También puede recibir este error:

```
SQL1032N No start database manager command was issued
```

Revise el archivo `db2diag.log` en busca de información diagnóstica que tenga que ver con este tipo de error.

Un ejemplo desde `db2diag.log`:

```
2011-04-26-16.04.11.820963-420 I2345542E1168       LEVEL: Error
PID     : 25178                TID  : 47207843621184PROC : db2sysc 0
INSTANCE: hannigan             NODE : 000
EDUID   : 1                    EDUNAME: db2sysc 0
FUNCTION: DB2 Common, OSSe, OSSHLibrary::load, probe:80
MESSAGE : ECF=0x90000076=-1879048074=ECF_LIB_CANNOT_LOAD
          Cannot load the specified library
DATA #1 : Hex integer, 4 bytes
0x00000002
DATA #2 : String, 58 bytes
/home/hannigan/sqllib/security64/plugin/server/dsmdb2pw.so
CALLSTCK:
  [0] 0x00002AEF63DD267E pdOSSeLoggingCallback + 0x20C
  [1] 0x00002AEF68486A42 /home/hannigan/sqllib/lib64/libdb2osse.so.1 + 0x1C4A42
  [2] 0x00002AEF6848825E ossLog + 0xA6
  [3] 0x00002AEF684928E9 _ZN11OSSHLibrary4loadEPKcm + 0x1D3
  [4] 0x00002AEF63F63BDC _Z20secLoadPluginGenericP19SEC_PLUGIN_HANDLE_TPc + 0x68
  [5] 0x00002AEF63F62FBB _Z23secLoadServerAuthPluginP19SEC_PLUGIN_HANDLE + 0x57
  [6] 0x00002AEF63F6C833 _Z25sqlexLoadAllPluginsServerP5sqlca + 0x3B5
```

```
  [7] 0x00002AEF6431737C /home/hannigan/sqllib/lib64/libdb2e.so.1 + 0x123637C
  [8] 0x00002AEF643164C5 sqloRunInstance + 0x191
  [9] 0x000000000040D31D DB2main + 0xD41

2011-04-26-16.04.11.825930-420 I2346711E1178       LEVEL: Error
PID     : 25178                TID  : 47207843621184PROC : db2sysc 0
INSTANCE: hannigan             NODE : 000
EDUID   : 1                    EDUNAME: db2sysc 0
FUNCTION: DB2 Common, OSSe, OSSHLibrary::load, probe:90
MESSAGE : ECF=0x90000076=-1879048074=ECF_LIB_CANNOT_LOAD
          Cannot load the specified library
DATA #1 : String, 109 bytes
../shared/gskit8/lib/linux64_x86/libgsk8iccs_64.so: cannot open shared object
file: No such file or directory
CALLSTCK:
  [0] 0x00002AEF63DD267E pdOSSeLoggingCallback + 0x20C
  [1] 0x00002AEF68486A42 /home/hannigan/sqllib/lib64/libdb2osse.so.1 + 0x1C4A42
  [2] 0x00002AEF6848825E ossLog + 0xA6
  [3] 0x00002AEF6849294D _ZN11OSSHLibrary4loadEPKcm + 0x237
  [4] 0x00002AEF63F63BDC _Z20secLoadPluginGenericP19SEC_PLUGIN_HANDLE_TPc + 0x68
  [5] 0x00002AEF63F62FBB _Z23secLoadServerAuthPluginP19SEC_PLUGIN_HANDLE + 0x57
  [6] 0x00002AEF63F6C833 _Z25sqlexLoadAllPluginsServerP5sqlca + 0x3B5
  [7] 0x00002AEF6431737C /home/hannigan/sqllib/lib64/libdb2e.so.1 + 0x123637C
  [8] 0x00002AEF643164C5 sqloRunInstance + 0x191
  [9] 0x000000000040D31D DB2main + 0xD41
```

Durante el inicio, el servidor detectará estos tipos de errores e intentará eliminar el complemento desde la configuración. Si el servidor no puede eliminar el complemento, debe eliminarlo desde la configuración del gestor de base de datos. Este mandato elimina el complemento desde la configuración del gestor de base de datos:

```
db2 get database manager configuration | grep SRVCON_PW_PLUGIN
db2 update database manager configuration using SRVCON_PW_PLUGIN \"\"
```

Rastreo del complemento de ID de usuario y contraseña

Si se configura correctamente, el servidor puede rastrear automáticamente el ID de usuario y el complemento de la contraseña (`dsmdb2pw`).

Para configurar el rastreo automático para el complemento de ID de usuario y contraseña, siga estos pasos:

AIX Linux

1. Asegúrese de que el servidor tenga autorización de escritura sobre el directorio `~/sqllib/db2dump/`.
2. Añada el texto siguiente al archivo `~instance/sqllib/userprofile`:

   ```
   export DB2_DSMDB2PW_TRACEFILE=filename
   ```

   donde *filename* es la vía de acceso completa y el nombre del archivo de rastreo, como por ejemplo `~/sqllib/db2dump/dsmdb2pw.trc`.
3. Reinicie DB2

Después de que se reinicie DB2, la salida del rastreo se guarda en el archivo y directorio especificados.

Windows

1. Para verificar que `DB2_VENDOR_INI db2set` está establecido, ejecute el mandato `db2set`.

2. Si la variable *DB2_VENDOR_INI* no está establecida, cree un archivo de configuración, como por ejemplo:
   ```
   c:\Program Files\Tivoli\TSM\s1\tsmdbmgr.env
   ```
3. Actualice el archivo de configuración que se muestra en *DB2_VENDOR_INI* con la ubicación del archivo de rastreo:
   ```
   DB2_DSMDB2PW_TRACEFILE=c:\Program Files\Tivoli\TSM\s1\sqllib\dsmdb2pw.trc
   ```
4. Configure el archivo de rastreo con el siguiente mandato:
   ```
   db2set -i server_instance DB2_VENDOR_INI=configuration_file_location
   ```

   por ejemplo:
   ```
   db2set -i s1 DB2_VENDOR_INI=c:\Program Files\Tivoli\TSM\s1\tsmdbmgr.env
   ```
5. Detenga el servidor de IBM Spectrum Protect y reinícielo con los siguientes mandatos:
   ```
   halt
   dsmserv -k server_instance
   ```

Después de que se reinicie el servidor, la salida del rastreo se guarda en el archivo y directorio especificados.

Consejo: Puede utilizar el nombre de archivo y el directorio que desee como nombre y ubicación del archivo de rastreo.

Limitación de la asignación de memoria de DB2

Cuando DB2 utiliza una gran cantidad de memoria, puede limitar la cantidad de memoria queDB2 utiliza emitiendo el mandato **db2 update**.

Acerca de esta tarea

De forma predeterminada, DB2 está instalado y configurado para utilizar la gestión de memoria automática, que hace que DB2 utilice un gran porcentaje de la memoria física. Para restringir la cantidad de memoria, utilice el mandato **db2 update** para especificar el límite de memoria.

Procedimiento

Emita el mandato **db2 update**:

```
db2 update dbm cfg using instance_memory memory_value
```

donde *memory_value* se especifica en bloques de 4 KB.

Ejemplo

Para limitar la asignación de memoria de DB2 para utilizar 3 200 000 KB de memoria, divida 3 200 000 KB en bloques de 4 KB, que da un resultado de 800 000. Después, emita el siguiente mandato:

```
db2 update dbm cfg using instance_memory 800000
```

Para obtener más información sobre la configuración de la memoria de instancia, consulte la Información sobre el producto DB2.

Recuperación de la información de la versión de DB2

La versión de DB2 que está instalada con el servidor de IBM Spectrum Protect se actualiza periódicamente. Si se producen problemas relacionados con la base de datos, debe saber cuál es la versión de DB2 y qué ubicación tiene para poder proporcionar esta información a IBM Software Support.

Procedimiento

Emita el mandato **db2level** para mostrar dónde están instalados los productos de DB2 en el servidor, y para listar el nivel de productos de DB2.
La siguiente salida muestra los resultados de ejemplo del mandato **db2level**.

AIX Linux

```
> db2level
DB21085I This instance or install (instance name, where applicable:
"cetinst1") uses "64" bits and DB2 code release "SQL10051" with level
identifier "0602010E".
Informational tokens are "DB2 v10.5.0.1", "special_31150",
"IP23526_31150", and Fix Pack "1".
Product is installed at "/opt/tivoli/tsm/db2".
```

Windows

```
C:\>db2level
DB21085I  This instance or install (instance name, where applicable: "SERVER1")
uses "64" bits and DB2 code release "SQL10051" with level identifier
"0602010E".
Informational tokens are "DB2 v10.5.100.64", "special_31150",
 "IP23521_31155", and Fix Pack "1".
Product is installed at "C:\PROGRA~1\Tivoli\TSM\db2" with DB2 Copy Name "DB2TSM1".
```

Ubicación de los archivos de registro de diagnóstico de DB2

El archivo `db2diag.log` contiene información diagnóstica que le puede ayudar a resolver problemas que se pueden producir con la base de datos.

La ubicación del archivo `db2diag.log` y los archivos FODC (first occurrence data capture) de DB2 depende de los valores de configuración de DB2 o de los valores de la variable de entorno de DB2. DB2 graba mensajes sobre operaciones internas, eventos o estado en el archivo de registro de notificaciones de administración (`db2SID.nfy`).

AIX Linux Realice los pasos siguientes para determinar dónde se ubica la vía de acceso de directorio de datos de diagnóstico:

1. Inicie la sesión como la instancia del usuario del servidor.
2. Emita el siguiente mandato:

   ```
   db2 get dbm cfg | grep DIAGPATH
   ```

   Si no se ha especificado ninguna vía de acceso en el parámetro de configuración de **DIAGPATH**, el directorio de datos de diagnóstico se encontrará en el subdirectorio `sqllib/db2dump` del directorio de instancias. Por ejemplo, `/home/tsminst1/sqllib/db2dump` donde `/home/tsminst1` es el directorio inicial de instancias.

Windows Realice los pasos siguientes para determinar dónde se ubica la vía de acceso de directorio de datos de diagnóstico:

1. Detenga la modalidad interactiva de DB2. Inicie una indicación de línea de mandatos de DB2 y emita el mandato `quit`.

2. Encuentre la vía de acceso utilizando el parámetro de configuración **DIAGPATH**. Emita el mandato

   ```
   db2 get dbm cfg | findstr /s /i diagpath
   ```

3. Si no se ha especificado ninguna vía de acceso en el parámetro de configuración **DIAGPATH**, se utilizará la vía de acceso del directorio de DB2INSTPROF. Busque la vía de acceso que se configuró en la variable de entorno *DB2INSTPROF*. Emita el siguiente mandato desde el indicador de línea de mandatos de DB2:

   ```
   db2set db2instprof
   ```

   La salida de este mandato muestra la ubicación de los archivos de datos de DB2. El archivo de registro de diagnóstico está en el subdirectorio de instancia que se especifica en la variable de registro*DB2INSTPROF*. Por ejemplo, para la instancia del servidor TSMSERVER1, el mandato **db2set deb2instprof** muestra esta vía de acceso:

   ```
   C:\ProgramData\IBM\DB2\DB2TSM1
   ```

   El archivo de registro de diagnóstico está en el subdirectorio TSMSERVER1:

   ```
   C:\ProgramData\IBM\DB2\DB2TSM1\TSMSERVER1
   ```

4. Si la variable de entorno *DB2INSTPROF* no se ha establecido, se utiliza x:\SQLLIB\DB2INSTANCE. x:\SQLLIB es la referencia de la unidad y también el directorio que se especifica en la variable de registro *DB2PATH*. El valor de *DB2INSTANCE* es el nombre de la instancia. No tiene que realizar la llamada al directorio SQLLIB. La primera parte de la salida desde el mandato **db2set db2path** es la vía de acceso al directorio de datos con el nombre de instancia añadido. La salida muestra la siguiente vía de acceso al directorio:

   ```
   C:\Program Files\Tivoli\TSM\db2\TSMINST1
   ```

   donde*DB2PATH* es C:\Program Files\Tivoli\TSM\db2 y el nombre de la instancia es TSMINST1.

Referencia relacionada:

"Archivos de registro de instalación" en la página 64

Archivos de registro actualizados de DB2

Cuando actualiza el servidor de IBM Spectrum Protect, el script DB2 **db2ckupgrade** ejecuta y crea archivos de registro para las bases de datos del servidor.

Durante la actualización, el asistente arregla de forma automática algunos error en la base de datos. Debe arreglar otros errores de forma manual. Compruebe los archivos de registro para conocer los errores que debe arreglar. Los archivos de registro contienen los resultados del mandato **db2ckupgrade** para cada base de datos.

Durante una actualización se crean los siguientes archivos de registro:

- AIX Linux /tmp/db2ckupgrade_*instance_name_db_name*.log
- Windows *installation_directory*\db2ckupgrade_*instance_name_db_name*.log

Si recibe un mensaje de error de la base de datos cuando está ejecutando el script que el asistente no arregla, debe cancelar o cerrar el asistente, arreglar el error e iniciar la actualización de nuevo. Si se trata de una actualización silenciosa que se está completando, debe comprobar el archivo log.text y buscar los errores, arreglar cualquier error que contenga el archivo e iniciar la actualización de nuevo. Para obtener más detalles sobre los mensajes de error que se listan en los archivos

de registro, consulte la Información sobre el producto DB2.

Resolución de un problema con un archivo de ID de base de datos inexistente o incorrecto

Si restaura una base de datos en otro servidor después de un desastre, quizá no pueda restaurar el archivo del ID de la base de datos (`dsmserv.dbid`). Por tanto, el servidor de IBM Spectrum Protect, no podrá encontrar el archivo tras la operación de restauración, y no podrá iniciarse.

Después de actualizar desde Tivoli Storage Manager versión 6.1 a 6.2, es posible que tenga dificultades para restaurar las bases de datos de Tivoli Storage Manager V6.1. Tiene que iniciar el servidor de Tivoli Storage Manager V6.2 para generar una nueva imagen de copia de seguridad en DB2. Una vez inicializado el servidor de Tivoli Storage Manager V6.2, se iniciará automáticamente una copia de seguridad de base de datos. Cuando se complete la copia de seguridad, detenga el servidor y emita el mandato **RESTORE DB**. Si la copia de seguridad automática de la base de datos no se completa correctamente, resuelva el problema y emita el mandato **BACKUP DB**. Asegúrese de que se haya completado antes de emitir el mandato **RESTORE DB**.

Importante: Para que las copias de seguridad incrementales de la base de datos o las restauraciones de la base de datos sean correctas, debe contar con una imagen de copia de seguridad de base de datos adecuada generada por el servidor de Tivoli Storage Manager V6.2.

Si ha iniciado el servidor de Tivoli Storage Manager V6.2 y la copia de seguridad de la base de datos automática se ha completado correctamente, podrá descartar la base de datos antes de restaurarla. No debe descartar la base de datos inmediatamente tras la actualización a la versión 6.2. Si descarta la base de datos antes de que se genere la imagen de copia de seguridad, deberá volver a instalar el servidor de Tivoli Storage Manager V6.1 y restaurar la base de datos.

Si tiene que restaurar una base de datos de Tivoli Storage Manager V6.1 y la base de datos no existe, deberá restaurarla a través de Tivoli Storage Manager V6.1. A continuación, podrá actualizar a Tivoli Storage Manager V6.2.

Si falta el archivo `dbid`, o no es correcto, esto podría afectar al inicio del servidor tras una operación de restauración de base de datos.

Cuando se restaura una base de datos, el archivo de ID de base de datos debe permanecer sincronizado con la base de datos. Con Tivoli Storage Manager V6.2, si formatea la base de datos antes de restaurarla, el archivo del ID de base de datos cambia. Este cambio provoca una no coincidencia de fecha y hora en la base de datos e impide que se inicie el servidor.

Si detecta que el archivo de ID de la base de datos está causando errores en una operación de restauración, es posible que tenga que utilizar el parámetro -S (omitir comprobación de DB ID). El archivo `dsmserv.dbid` no debe estar presente en el servidor cuando se utiliza el parámetro -S. En las siguientes situaciones se describen los casos en los que resulta útil el parámetro -S:

- Si vuelve a formatear el servidor después de realizar una copia de seguridad del mismo, tendrá una no coincidencia de fecha y hora entre el nuevo archivo `dsmserv.dbid`. Utilice el parámetro -S cuando inicie el servidor después de una restauración.
- Cuando el archivo `dsmserv.dbid` se dañe o se pierda.

Tras el uso inicial del parámetro -S en un caso de ejemplo de restauración, el servidor crea un archivo `dsmserv.dbid` en el directorio de instancias.

Resolución de problemas con los mandatos BACKUP DB y RESTORE DB

Los mandatos **BACKUP DB** y **RESTORE DB** del servidor requieren que la aplicación de base de datos DB2 de IBM realice una copia de seguridad de la base de datos de IBM Spectrum Protect en el servidor.

A continuación los datos de la copia de seguridad se envían al servidor a través de la interfaz de programación de aplicaciones (API) del cliente.

Cuando falle un mandato **BACKUP DB** o **RESTORE DB** con un mensaje DB2 SQLCODE o SQLERRMC con códigos de retorno, siga estos procedimientos para obtener una descripción del DB2 SQLCODE:

1. Abra una interfaz de línea de mandatos DB2:

   Windows Para Windows, pulse **Inicio** > **Todos los programas** > **IBM DB2** y a continuación, pulse **Herramientas de línea de mandatos** > **Procesador de línea de mandatos**.

   AIX Linux En el resto de plataformas compatibles, conéctese con el ID de instancia de DB2, abra una ventana de shell y emita el mandato `DB2`.
2. Especifique el SQLCODE. Por ejemplo, si el DB2 SQLCODE es -2033, emita el siguiente mandato:

   ```
   ? sql2033
   ```

Puede utilizar los detalles de la condición del error para depurar el problema con el mandato **BACKUP DB** o **RESTORE DB**. Si el código SQLERRMC se muestra también, su explicación se encuentra en la descripción de SQLCODE suministrada a los usuarios. Podrá encontrar más información acerca de los códigos de retorno de la API en los siguientes archivos:

- Windows `tsm\api\include\dsmrc.h`
- AIX Linux `tsm/client/api/bin64/sample/dsmrc.h`

Resolución de variables de entorno incorrectas para BACKUP DB y RESTORE DB

Muchos de los problemas de proceso de **BACKUP DB** o **RESTORE DB** son resultado de una configuración incorrecta de las variables de entorno DSMI_CONFIG, DSMI_DIR o DSMI_LOG.

Acerca de esta tarea

Requisito:
La API del cliente utiliza las variables de entorno para localizar los códigos de API y los archivos de opciones. La instancia DB2 debe ejecutarse en un shell con las variables de entorno correctamente configuradas.

AIX Linux Las variables DSMI_* se definen en el archivo de `userprofile` de la instancia. Por ejemplo: `/home/tsminst1/sqllib/userprofile`

Windows Las variables DSMI_* se ajustan en el archivo al que hace referencia la variable de registro de la instancia de DB2, DB2_VENDOR_INI. Por ejemplo, este

archivo puede ser c:\tsminst1\tsmdbmgr.env. Puede verificar el nombre y ubicación del archivo emitiendo el mandato db2set -i tsminst1 DB2_VENDOR_INI, donde tsminst1 es la instancia de DB2.

Las variables DSMI_* son configuradas inicialmente de forma automática por el asistente para la configuración de instancias de IBM Spectrum Protect.

Procedimiento

Abra el archivo /home/tsminst1/sqllib/userprofile y revise las sentencias. Si cambia este archivo, detenga y reinicie la instancia de DB2 para que se incluyan los cambios. Por ejemplo, piense en el siguiente caso de ejemplo. El archivo userprofile tiene sentencias como el siguiente texto de ejemplo:

```
export DSMI_CONFIG=server_instance_directory/tsmdbmgr.opt
export DSMI_DIR=server_bin_directory/dbbkapi
export DSMI_LOG=server_instance_directory
```

El archivo tsmdbmgr.opt tiene el siguiente texto:

```
SERVERNAME TSMDBMGR_TSMINST1
```

El archivo *server_bin_directory*/dbbkapi/dsm.sys tiene el siguiente texto:

```
SERVERNAME TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
errorlogname /tsminst1/tsmdbmgr.log
```

Compruebe que la entrada SERVERNAME del archivo tsmdbmgr.opt coincide con la entrada SERVERNAME del archivo dsm.sys.

Linux No añada la opción de generación de PASSWORDACCESS al archivo de configuración dsm.sys. Esta opción puede hacer que la base de datos falle.

Resolución del mensaje de error ANR2968E

El mensaje de error ANR2968E se muestra durante el mandato **BACKUP DB**.

Acerca de esta tarea

Hay dos causas para este mensaje de error:

- Si el archivo de anotaciones de error de IBM Spectrum Protect es propiedad del ID de usuario raíz en lugar del ID de usuario de la instancia del servidor.
- Windows Si utiliza comillas simples para rodear a las vías de acceso que se encuentran en el archivo tsmdbmgr.env. Utilice una vía de acceso que no contenga espacios o utilice el nombre abreviado de Windows para la vía de acceso.

Para corregir el error causado por el ID de usuario raíz, realice los pasos siguientes:

Procedimiento

1. Inicie la sesión utilizando un ID de instancia de servidor de IBM Spectrum Protect y verifique el nombre del archivo de registro de errores. Por ejemplo:

   ```
   $ grep -i "ERRORLOGNAME" $DSMI_DIR/dsm.sys
   ERRORLOGNAME /home/db2inst1/tsminst1/tsmdbmgr.log
   ```

   donde db2inst1 es el ID de usuario de instancia del servidor y /home/db2inst1/tsminst1/ es el directorio de instancia del servidor.

2. Emita el siguiente mandato de ejemplo para verificar el propietario actual del archivo de registro de errores:

   ```
   $ ls -la /home/db2inst1/tsminst1/tsmdbmgr.log
   -rw-r--r-- 1 root system 834 May 05 09:43 /home/db2inst1/tsminst1/tsmdbmgr.log
   ```

3. Si el archivo de anotaciones de errores no es propiedad del ID de usuario de instancia de IBM Spectrum Protect, elimínelo. Debe tener autorización root para eliminar el archivo. Emita el siguiente mandato de ejemplo para eliminar el archivo de anotaciones:

   ```
   $ su contraseña raíz
   # rm /home/db2inst1/tsminst1/tsmdbmgr.log
   # exit
   ```

4. Emita el mandato **BACKUP DB** y verifique que el mandato se ha completado satisfactoriamente. Verifique que el archivo de registro es propiedad del ID de instancia del servidor. Por ejemplo:

   ```
   $ ls -la /home/db2inst1/tsminst1/tsmdbmgr.log
   -rw-r--r-- 1 db2inst1 db2iadm1 834 May 05 09:50
   /home/db2inst1/tsminst1/tsmdbmgr.log
   ```

Resolución del mensaje de error ANR2971E mediante el código SQL

El mensaje de error ANR2971E puede mostrarse cuando se detiene el proceso durante una operación de copia de seguridad o restauración de la base de datos. Utilice el código SQL asociado al error para intentar resolver este problema.

Antes de empezar

Si va a restaurar una base de datos porque el servidor se detuvo durante una operación normal, revise el archivo `db2diag.log` *antes* de ejecutar la operación de copia de seguridad o restauración.

Es posible que aparezca el siguiente mensaje cuando se va a restaurar o hacer una copia de seguridad de los datos:

```
ANR2971E Ha finalizado la copia de seguridad/restauración/rollforward
de la base de datos - DB2 sqlcode -2581 error
```

En el siguiente caso de ejemplo, el proceso **DSMSERV RESTORE DB** ha fallado con el código de SQL 2581 para DB2. El caso de ejemplo que se presenta a continuación no pertenece a problemas con las variables de entorno DSMI.

Procedimiento

1. Emita el siguiente mandato desde la interfaz de línea de mandatos de DB2:

   ```
   ? SQL2581
   ```

   Se genera una explicación acerca del código de SQL.

   ```
   SQL2581N  Restore is unable to extract log files or restore a log
   directory from the backup image to the specified path. Reason code 2581
   ```

2. Examine el archivo `db2diag.log`, donde podrá encontrar mensajes de error y de estado. En el siguiente ejemplo, se muestra una parte del archivo `db2diag.log`:

   ```
   2009-02-10-09.49.00.660000-300 E8120712F500       LEVEL: Info
   PID     : 4608                 TID  : 3956        PROC : db2syscs.exe
   INSTANCE: SERVER1              NODE : 000         DB   : TSMDB1
   APPHDL  : 0-7                  APPID: *LOCAL.SERVER1.090210144859
   AUTHID  : B1JRPM01
   EDUID   : 3956                 EDUNAME: db2agent (TSMDB1)
   FUNCTION: DB2 UDB, database utilities, sqludPrintStartingMsg, probe:1292
   DATA #1 : <preformatted>
   ```

```
Starting a full database restore.
Agent EDU ID: 3956

2009-02-10-09.50.21.051000-300 E8123213F483       LEVEL: Severe
PID     : 4608                 TID  : 5080        PROC : db2syscs.exe
INSTANCE: SERVER1              NODE : 000
EDUID   : 5080                 EDUNAME: db2bm.3956.1 (TSMDB1)
FUNCTION: DB2 UDB, database utilities, sqluWriteLogFile, probe:1498
MESSAGE : ZRC=0x850F000C=-2062614516=SQLO_DISK "Disk full."
            DIA8312C Disk was full.
DATA #1 : String, 46 bytes
F:\tivoli\tsm\Beta\sarch\RstDbLog\S0000262.LOG

2009-02-10-09.50.21.051000-300 E8124165F912       LEVEL: Severe
PID     : 4608                 TID  : 5080        PROC : db2syscs.exe
INSTANCE: SERVER1              NODE : 000
EDUID   : 5080                 EDUNAME: db2bm.3956.1 (TSMDB1)
FUNCTION: DB2 UDB, database utilities, sqluWriteLogFile, probe:1500
MESSAGE : SQL2581N  Restore is unable to extract log files or restore a log
          directory from the backup image to the specified path. Reason code "".
DATA #1 : SQLCA, PD_DB2_TYPE_SQLCA, 136 bytes
sqlcaid : SQLCA     sqlcabc: 136   sqlcode: -2581   sqlerrml: 1
sqlerrmc: 4
sqlerrp : sqluWrit
sqlerrd : (1) 0x00000000      (2) 0x00000000      (3) 0x00000000
          (4) 0x00000000      (5) 0x00000000      (6) 0x00000000
sqlwarn : (1)      (2)      (3)      (4)        (5)       (6)
          (7)      (8)      (9)      (10)        (11)
sqlstate:
```

En el ejemplo anterior, podemos ver a través del mensaje “Disco lleno”, que no había suficiente espacio en el disco para situar los archivos de registro necesarios de la operación de copia de seguridad.

3. Añada espacio de disco y vuelva a ejecutar la operación.

Errores comunes de BACKUP DB y RESTORE DB

Los errores comunes derivados de los mandatos **BACKUP DB** o **RESTORE DB** pueden incluir códigos de error o de retorno de SQL.

A continuación, figuran los errores que aparecen con más frecuencia cuando emite los mandatos **BACKUP DB** o **RESTORE DB**.

ANR2968E - Ha finalizado la copia de seguridad de la base de datos DB2 SQLCODE -2033 SQLERRMC 406

Para resolver el mensaje de error SQL 406, asegúrese de que los siguientes problemas se han resuelto:

- La variable de entorno DSMI_CONFIG debe señalar a un archivo de opciones de IBM Spectrum Protect válido.
- El propietario de la instancia debe tener acceso de lectura al archivo `dsm.opt`.
- La variable del entorno DSMI_CONFIG se define como `~/sqllib/userprofile` y `~/sqllib/usercshrc`.

DB2 SQLCODE: -2033, DB2 SQLERRMC: 106

Si recibe un mensaje de error SQL 106, significa que hay un problema de permisos con el archivo de registro que graba la interfaz de programación de la aplicación (API) para el cliente.

Para resolver el error, encuentre el archivo de registro con el problema de permisos, inicie sesión con el ID de usuario raíz y borre el archivo.

DB2 SQLCODE: -2033, DB2 SQLERRMC: 168

Verifique que la variable de entorno DSMI_DIR apunta al directorio ejecutable de la API del cliente que contiene el agente de comunicación de confianza `dsmtca`.

ANR2971E - Ha finalizado la copia de seguridad/restauración/ rollforward de la base de datos DB2 SQLCODE - Error 2071

La biblioteca no se puede cargar porque la biblioteca o una biblioteca que esta necesita no existe o no tiene un formato válido. Si la biblioteca no se puede cargar, quiere decir que se está cargando una biblioteca de 32 bits en una instancia de 64 bits, o que una biblioteca de 64 bits se está cargando en una instancia de 32 bits. Si no se puede cargar una biblioteca, también indica que la variable de entorno DSMI_DIR apunta a los archivos ejecutables de la API de cliente de IBM Spectrum Protect equivocados. Para obtener información sobre el error, abra una ventana del procesador de línea de mandatos de DB2 y emita el siguiente mandato:

```
db2 => ? sql2071
```

Asegúrese de que si se ha realizado algún cambio en los archivos `tsmdbmgr.opt`, `dsm.sys` o `sqllib/userprofile`, se recicle la instancia de DB2 para que adopte los nuevos valores. Para reciclar la instancia de DB2, detenga e inicie el servidor de IBM Spectrum Protect. Además, verifique que el mandato **EXPORT** preceda a las entradas `DSMI_*=` del archivo `sqllib/userprofile`.

El mensaje de error indica que el nodo está bloqueado

Es posible que reciba un error cuando DB2 se ponga en contacto con un servidor y un nodo particular reciba un mensaje de error que quiere decir que el nodo está bloqueado.

Para corregir el error, utilice la dirección de localhost en vez de una dirección de bucle de retorno explícita, por ejemplo 127.0.0.1. Especifique la opción `tcpserveraddress localhost` en la stanza SERVERNAME TSMDBMGR_TSMINST1 del archivo `dsm.sys`.

Problemas con el rendimiento de copia de seguridad de la base de datos

En algunos casos, en particular en los sistemas de AIX, si el servidor está configurado para utilizar TCP/IP para la copia de seguridad de la base de datos y las operaciones de restauración, es posible que las copias de seguridad de la base de datos se vean ralentizadas. Para resolver el problema, configure la instancia del servidor para utilizar la memoria compartida.

Tareas relacionadas:

"Configuración de una instancia de servidor para utilizar la memoria compartida" en la página 60

Características del ID de usuario $$_TSMDBMGR_$$

El servidor de IBM Spectrum Protect genera el ID de usuario $$_TSMDBMGR_$$ al inicio.

Puede visualizar el ID de usuario $$_TSMDBMGR_$$ en los resultados de un mandato **QUERY SESSION**. Este ID también está presente en el archivo de registro de actividad y en otros archivos de registro de servidor.

El servidor utiliza el ID de usuario de $$_TSMDBMGR_$$ para realizar una copia de seguridad de la base de datos del servidor. Al utilizar el ID de usuario de $$_TSMDBMGR_$$, puede hacer la base de datos accesible para procesarla si el servidor no está disponible. El cambio de este ID perjudica la capacidad de recuperación o restauración de un servidor si se produce un desastre.

Restricción: No podrá cambiar el archivo `dsm.sys` o `dsm.opt` para configurar o utilizar un nombre de nodo de cliente distinto. La base de datos de servidor local de IBM Spectrum Protect utiliza el archivo `dsm.sys` o `dsm.opt` para realizar una copia de seguridad de su propia base de datos.

Resolución de problemas de reorganización de la base de datos

La reorganización de tablas de base de datos y la reorganización de índices requieren una cantidad significativa de recursos del sistema. Para evitar ocupar recursos del sistema que se puedan utilizar en otro lugar, ejecute las rutinas de reorganización en momentos de desactivación.

Se puede producir el crecimiento de base de datos inesperado y requisitos de espacio de anotaciones de archivado y activo inesperado si las tablas o los índices asociados con las tablas no se han reorganizado. IBM Spectrum Protect reorganiza las tablas de forma predeterminada. Si la reorganización automática está afectando al rendimiento del servidor, puede planificar manualmente la reorganización.

Las siguientes sugerencias pueden ayudar al configurar la reorganización:

- Active la reorganización del índice si está ejecutando la deduplicación en el servidor. Consulte la opción del servidor `ALLOWREORGINDEX`.
- De manera predeterminada, la reorganización de tablas se activa 24 horas al día. Ejecute la reorganización durante una hora del día relativamente inactiva. Consulte las siguientes opciones del servidor para definir una hora inactiva cuando se pueda ejecutar la reorganización:
  - `REORGBEGINTIME`
  - `REORGDURATION`

Análisis de los síntomas del proceso para resolver problemas

Puede determinar en ocasiones la causa de los errores observando los síntomas del proceso.

Es posible que encuentre uno de los siguientes síntomas del proceso:

- Espacio insuficiente en una agrupación de almacenamiento de copia de destino
- La detección de un archivo dañado en el volumen
- No se da caducidad a los archivos después de haber reducido el número de versiones que deben conservarse

- La migración no se ejecuta para una agrupación de almacenamiento de medios secuenciales
- La migración sólo utiliza un proceso
- El proceso se ejecuta con lentitud

Revisión de los mensajes de proceso para determinar el estado de las operaciones del servidor

Los procesos del servidor, independientemente de si se ejecutan en primer plano o en segundo plano, emitirán siempre un mensaje de "proceso iniciado" y otro de "proceso finalizado" además de los mensajes de proceso generales. Puede utilizar estos mensajes para determinar el estado de las operaciones del servidor.

Procesos que se ejecutan en el servidor

Un proceso de servidor es una tarea que se realiza en el servidor. Puede asignar la tarea para realizar una operación específica, como migrar datos desde una agrupación de almacenamiento hasta la siguiente en la jerarquía. Emita el servidor para resolver los problemas que tenga con el servidor.

Los procesos de servidor a menudo se inician como proceso automático en el servidor. El proceso puede verse o no afectado por una opción del servidor u otro valor. El proceso de servidor también puede ser iniciado por un mandato.

La mayoría de los procesos de servidor pueden ejecutarse en primer plano o de forma síncrona. Los procesos que se ejecutan en primer plano pueden iniciarse mediante la emisión de un mandato con el parámetro WAIT=YES. Los mandatos que inician procesos de servidor y no admiten el parámetro WAIT=YES o los que se especifican con WAIT=NO se ejecutan en modalidad BACKGROUND o de forma asíncrona.

Algunos procesos de servidor pueden iniciar simultáneamente varios procesos para llevar a cabo la tarea. Consulte Tabla 7 para conocer las descripciones de los procesos del servidor.

Tabla 7. Procesos del servidor

Proceso o mandato	Descripción	Se ejecuta en primer plano o como un proceso múltiple
AUDIT VOLUME	Se utiliza para auditar el contenido de un volumen para validar que los datos que todavía pueden leerse y que las definiciones de base de datos de servidor que describen los datos son correctos.	
BACKUP DB	Se utiliza para realizar la copia de seguridad de la base de datos del servidor (completa o incremental).	BACKUP DB puede ejecutarse como proceso síncrono especificando WAIT=YES.

Tabla 7. Procesos del servidor (continuación)

Proceso o mandato	Descripción	Se ejecuta en primer plano o como un proceso múltiple
BACKUP STGPOOL	La copia de seguridad de una agrupación de almacenamiento primaria se realiza en una agrupación de almacenamiento de copia. Se utiliza para realizar copias duplicadas de los datos y, potencialmente, traspasar copias duplicadas a una ubicación fuera del local.	El mandato **BACKUP STGPOOL** puede ejecutarse como un proceso sincronizado especificando **WAIT=YES**. **BACKUP STGPOOL** podría ejecutarse únicamente utilizando diversos procesos simultáneos, controlados por el parámetro **MAXPROCESS** especificado en el mandato **BACKUP STGPOOL**.
CHECKIN LIBVOLUME	Se utiliza para dar de alta un volumen de cinta en una biblioteca de cintas.	
CHECKOUT LIBVOLUME	Se utiliza para dar de baja un volumen de cinta de una biblioteca de cintas.	
Caducidad	Elimina los archivos de copia de seguridad y archivado del servidor en función de las políticas definidas para gestionar dichos archivos. Puede ejecutar la caducidad de forma automática especificando EXPINTERVAL=*n* en el archivo de opciones del servidor, donde *n* es un número distinto de cero. La caducidad también puede iniciarse emitiendo el mandato **EXPIRE INVENTORY**. No es posible que más de un proceso de caducidad se ejecute a la vez, aunque puede ejecutar más de un subproceso al mismo tiempo.	El mandato **EXPIRATION** puede ejecutarse como un proceso sincronizado especificando WAIT=YES.
IMPORT	Se utiliza para importar datos desde volúmenes de medios secuenciales o directamente desde otro servidor utilizando las conexiones de la comunicación TCP/IP entre los servidores. El proceso de importación lo puede iniciar cualquiera de los siguientes mandatos: • **IMPORT ADMIN** • **IMPORT NODE** • **IMPORT POLICY** • **IMPORT SERVER**	
LABEL LIBVOLUME	Se utiliza para etiquetar uno o varios volúmenes de biblioteca en una biblioteca.	

Tabla 7. Procesos del servidor (continuación)

Proceso o mandato	Descripción	Se ejecuta en primer plano o como un proceso múltiple
Migration	Se utiliza para migrar datos desde una agrupación de almacenamiento hasta la siguiente agrupación de almacenamiento de la jerarquía de almacenamiento. La migración se inicia y se detiene en función de los umbrales HighMig y LowMig que se han definido para la agrupación de almacenamiento. Siempre que se emite **UPDATE STGPOOL**, estos valores vuelven a examinarse y, si corresponde, se inicia **MIGRATION**. De lo contrario, el servidor supervisa el porcentaje de utilización para los datos no migrados de una agrupación de almacenamiento. De ser necesario, inicia el proceso de migración para esa agrupación de almacenamiento cuando se ha excedido el umbral de HighMig. También puede emitir el mandato **MIGRATE STGPOOL** para iniciar de forma manual el proceso de migración.	La migración puede configurarse para ejecutar varios procesos simultáneos. Los procesos múltiples se controla mediante el atributo MIGPROCESS de la agrupación de almacenamiento y pueden actualizarse emitiendo el mandato **UPDATE STGPOOL**.
MOVE DATA	Se utiliza para traspasar datos desde un volumen hasta otros volúmenes de la misma agrupación de almacenamiento o hasta una agrupación de almacenamiento distinta.	El mandato **MOVE DATA** puede ejecutarse como un proceso sincronizado especificando WAIT=YES.
MOVE DRMEDIA	Gestione los medios de recuperación ante siniestro traspasando los volúmenes dentro del sitio fuera de él o devolviendo los volúmenes fuera del sitio nuevamente a él. Los medios de recuperación ante siniestro son los volúmenes de copia de seguridad de base de datos y de copia de seguridad de agrupación de almacenamiento necesarios para proteger y recuperar el servidor.	El mandato **MOVE DRMEDIA** puede ejecutarse como un proceso sincronizado especificando WAIT=YES.
MOVE MEDIA	Se utiliza para traspasar volúmenes desde una biblioteca de cintas hasta la ubicación de desbordamiento para impedir que una biblioteca pueda llenarse.	
MOVE NODEDATA	Se utiliza para traspasar todos los datos para el nodo o nodos especificados a otros volúmenes de la misma agrupación de almacenamiento o a una agrupación de almacenamiento distinta.	El mandato **MOVE NODEDATA** puede ejecutarse como un proceso sincronizado especificando WAIT=YES.

Tabla 7. Procesos del servidor (continuación)

Proceso o mandato	Descripción	Se ejecuta en primer plano o como un proceso múltiple
PREPARE	Se utiliza para crear un archivo de plan de recuperación.	El mandato **PREPARE** puede ejecutarse como un proceso sincronizado especificando WAIT=YES.
Reclamation	Se utiliza para reclamar espacio de los volúmenes de cinta traspasando los datos activos a otros volúmenes y estableciendo el volumen nuevamente como volumen vacío o privado o bien como volumen reutilizable. El servidor supervisa el **RECLAMATION THRESHOLD** definido para una agrupación de almacenamiento. Inicia un proceso de reclamación para esa agrupación de almacenamiento para reclamar cualquier volumen susceptible de reclamarse, si determina que existen uno o varios volúmenes susceptibles de reclamarse.	
RESTORE STGPOOL	Se utiliza para restaurar todos los archivos para una agrupación de almacenamiento determinada desde una agrupación de almacenamiento de copia.	El mandato **RESTORE STGPOOL** puede ejecutarse como un proceso sincronizado especificando WAIT=YES. **RESTORE STGPOOL** puede ejecutarse utilizando diversos procesos simultáneos, controlados por el parámetro **MAXPROCESS** especificado en el mandato **RESTORE STGPOOL**.
RESTORE VOLUME	Se utiliza para restaurar todos los archivos para un volumen determinado desde una agrupación de almacenamiento de copia.	El mandato **RESTORE VOLUME** puede ejecutarse como un proceso sincronizado especificando WAIT=YES. **RESTORE VOLUME** puede ejecutarse utilizando diversos procesos simultáneos, controlados por el parámetro **MAXPROCESS** especificado en el mandato **RESTORE VOLUME**.

Mensajes emitidos al iniciarse procesos

Cuando el servidor ejecuta tareas como procesos, a los procesos se les asigna un mensaje de identificación e informan de que se han iniciado.

El inicio del proceso se emite en el siguiente mensaje:

ANR0984I El proceso *id_proceso* de *nombre_proceso* se ha iniciado en el estado *estado_proceso* a las *hora*

La siguiente lista define las variables de este mensaje:

id_proceso
Identificador de proceso numérico.

nombre_proceso
El nombre del proceso.

estado_proceso
PRIMER PLANO o **SEGUNDO PLANO**. Si el proceso se ejecuta en primer plano, el mandato se ha emitido con el parámetro **WAIT=YES**. El proceso en primer plano hace que la sesión de administración que ha emitido el mandato espere hasta que el proceso finalice. Un proceso que se ejecuta en segundo plano vuelve inmediatamente a la sesión de administración que ha emitido el mandato, lo que indica que se ha iniciado un proceso mientras el proceso sigue en ejecución. Los procesos que se ejecutan en segundo plano pueden supervisarse mediante el mandato **QUERY PROCESS**.

hora La hora a la que se ha iniciado el proceso.

Mensajes emitidos al finalizar procesos

Cuando el servidor ejecuta tareas como procesos, los procesos informarán cuando finalicen. Los mensajes "proceso finalizado" que se emiten varían de proceso a proceso. El mensaje depende de si el proceso debe informar sobre elementos y bytes procesados, no elementos ni bytes procesados, elementos procesados, o sólo bytes procesados.

El proceso ha finalizado

Cuando un proceso se completa y no cuenta con ningún byte o número de archivos de los que debe informar, se emite el mandato siguiente:

ANR0985I El proceso *id_proceso* para *nombre_proceso* que se ejecuta en el estado *estado_proceso* se ha completado
con el estado *estado_terminación* a las *hora*

La siguiente lista define las variables de este mensaje:

id_proceso
Identificador de proceso numérico.

nombre_proceso
El nombre del proceso.

estado_proceso
PRIMER PLANO o **SEGUNDO PLANO**. Si el proceso se ejecuta en primer plano, el mandato se ha emitido con el parámetro **WAIT=YES**. El proceso en primer plano hace que la sesión de administración que ha emitido el mandato espere hasta que el proceso finalice. Un proceso que se ejecuta en segundo plano vuelve inmediatamente a la sesión de administración que ha emitido el mandato, lo que indica que se ha iniciado un proceso mientras el proceso sigue en ejecución. Los procesos que se ejecutan en segundo plano pueden supervisarse mediante el mandato **QUERY PROCESS**.

estado_terminación
Correcto o incorrecto.

hora La hora a la que se ha iniciado el proceso.

El proceso ha finalizado con elementos y bytes

Cuando un proceso se completa y cuenta con bytes y elementos procesados de los que debe informar, se emite el mandato siguiente:

```
ANR0986I El proceso id_proceso para nombre_proceso que
se ejecuta en el estado estado_proceso
ha procesado número_de_elementos de un total de bytes_procesados bytes con un
estado de terminación de estado_terminación a las hora
```

La siguiente lista define las variables de este mensaje:

id_proceso
Identificador de proceso numérico.

nombre_proceso
El nombre del proceso.

estado_proceso
PRIMER PLANO o **SEGUNDO PLANO**. Si el proceso se ejecuta en primer plano, el mandato se ha emitido con el parámetro **WAIT=YES**. El proceso en primer plano hace que la sesión de administración que ha emitido el mandato espere hasta que el proceso finalice. Un proceso que se ejecuta en segundo plano vuelve inmediatamente a la sesión de administración que ha emitido el mandato, lo que indica que se ha iniciado un proceso mientras el proceso sigue en ejecución. Los procesos que se ejecutan en segundo plano pueden supervisarse mediante el mandato **QUERY PROCESS**.

número_elementos
El número de elementos procesados.

bytes_procesados
El número de bytes procesados.

estado_terminación
Correcto o incorrecto.

hora La hora a la que se ha iniciado el proceso.

El proceso ha finalizado con elementos

Cuando un proceso se completa y cuenta con elementos procesados de los que debe informar, se emite el mandato siguiente:

```
ANR0987I El proceso id_proceso para nombre_proceso que se ejecuta en el estado
estado_proceso
ha procesado número_de_elementos elementos con un estado de terminación de
estado_terminación a las hora
```

La siguiente lista define las variables de este mensaje:

id_proceso
Identificador de proceso numérico.

nombre_proceso
El nombre del proceso.

estado_proceso
PRIMER PLANO o **SEGUNDO PLANO**. Si el proceso se ejecuta en primer plano, el

mandato se ha emitido con el parámetro **WAIT=YES**. El proceso en primer plano hace que la sesión de administración que ha emitido el mandato espere hasta que el proceso finalice. Un proceso que se ejecuta en segundo plano vuelve inmediatamente a la sesión de administración que ha emitido el mandato, lo que indica que se ha iniciado un proceso mientras el proceso sigue en ejecución. Los procesos que se ejecutan en segundo plano pueden supervisarse mediante el mandato **QUERY PROCESS**.

estado_terminación
Correcto o incorrecto.

hora La hora a la que se ha iniciado el proceso.

El proceso ha finalizado con bytes

Cuando un proceso se completa y cuenta con bytes procesados de los que debe informar, se emite el mandato siguiente:

```
ANR0988I El proceso id_proceso para nombre_proceso que se ejecuta
 en el estado estado_proceso
ha procesado bytes_procesados bytes con un estado de terminación
de estado_terminación a las hora
```

La siguiente lista define las variables de este mensaje:

id_proceso
Identificador de proceso numérico.

nombre_proceso
El nombre del proceso.

estado_proceso
PRIMER PLANO o **SEGUNDO PLANO**. Si el proceso se ejecuta en primer plano, el mandato se ha emitido con el parámetro **WAIT=YES**. El proceso en primer plano hace que la sesión de administración que ha emitido el mandato espere hasta que el proceso finalice. Un proceso que se ejecuta en segundo plano vuelve inmediatamente a la sesión de administración que ha emitido el mandato, lo que indica que se ha iniciado un proceso mientras el proceso sigue en ejecución. Los procesos que se ejecutan en segundo plano pueden supervisarse mediante el mandato **QUERY PROCESS**.

bytes_procesados
El número de bytes procesados.

estado_terminación
Correcto o incorrecto.

hora La hora a la que se ha iniciado el proceso.

Análisis del mensaje de error ANR1221E

Cuando reciba el mensaje de error ANR1221E, la causa se debe normalmente a un espacio insuficiente en la agrupación de almacenamiento de copia de destino.

Acerca de esta tarea

Realice los siguientes pasos para resolver el mensaje de error ANR1221E:

Procedimiento

1. Emita el mandato **QUERY STGPOOL** *nombre_agrupación_almacenamiento* **F=D**.

2. Emita la sentencia select de SQL desde un cliente de administración a este servidor: "`select nombre_agrupación_almacenamiento,nombre_clase_disp,recuento(*) as 'VOLUMES' from volumes group by nombre_agrupación_almacenamiento,nombre_clase_disp`."
3. Compare el número de volúmenes especificados por la sentencia select con los volúmenes máximos reutilizables permitidos (según lo especificado por el mandato **QUERY STGPOOL**). Si el número de volúmenes del que informa **select** es igual a o supera el "Número máximo de volúmenes reutilizables", actualice la agrupación de almacenamiento y permita más volúmenes reutilizables. Si los volúmenes reutilizables no se utilizan en la agrupación de almacenamiento (scratch=0), asegúrese de que agrega más volúmenes privados. Emita el mandato `UPDATE STGPOOL Nombreagrupaciónstg MAXSCR=nn`, donde *Nombreagrupaciónstg* es el nombre de la agrupación de almacenamiento a actualizar y *nn* es el número aumentado de volúmenes reutilizables para poder a disposición de esta agrupación de almacenamiento de copia.

   Importante: la biblioteca de cintas deben tener este número de volúmenes reutilizables adicionales disponible, o bien necesita añadir volúmenes reutilizables en la biblioteca antes de emitir este mandato y volver a intentar la operación **BACKUP STGPOOL**.

Análisis del mensaje de error ANR2317W

El mensaje de error ANR2317W se emite cuando un proceso determina que hay un archivo dañado.

Acerca de esta tarea

El mensaje se muestra con la información siguiente:

```
ANR2317W Audit Volume found damaged file on volume volumeName: Node nodeName,
Type fileType, File space fileSpaceName, fsId fileSpaceID,
File name fileName is number version of totalVersions versions.
```

Siga estos pasos para resolver el mensaje de error ANR2317W:

Procedimiento

1. Emita el mandato **QUERY VOLUME** *nombre_volumen* **F=D**.
2. Emita la sentencia select de SQL desde un cliente de administración a este servidor: "`select* from VOLHISTORY where VOLUME_NAME='volume_name' AND TYPE='STGNEW`." Los resultados del mandato **QUERY VOLUME** indican cuándo se escribió este volumen por última vez. La información de la operación **SELECT** indica cuándo se ha agregado este volumen a la agrupación de almacenamiento. A menudo, **AUDIT VOLUME** puede especificar archivos como dañados, porque, en el momento en el que se grabaron los datos, el hardware no funcionaba correctamente y no se grabaron los datos correctamente, aunque notificó al servidor de IBM Spectrum Protect que la operación había sido satisfactoria. Como resultado de este funcionamiento incorrecto de un dispositivo, puede que se hayan visto afectados muchos archivos de muchos volúmenes distintos. Siga estos pasos para corregir este problema:
   a. Evalúe las anotaciones de errores del sistema u otra información relacionada con esta unidad para determinar si todavía se informa de un error. Si todavía se informa de errores, primero deberán solucionarse éstos. Para solucionar un error de hardware, póngase en contacto con el proveedor del hardware para, conjuntamente, corregir el problema.

b. Si este volumen de agrupación de almacenamiento es una copia de otro, simplemente suprima este volumen utilizando el mandato **DELETE VOLUME** *nombre_volumen* **DISCARDDATA=YES**. La próxima vez que se ejecute una copia de seguridad de agrupación de almacenamiento para la agrupación o agrupaciones de almacenamiento primarias en las que residen los datos dañados, volverá a realizarse la copia de seguridad de ésta en esta agrupación de almacenamiento de copia y no será necesario realizar ninguna acción adicional.
   - Si este volumen de agrupación de almacenamiento es un volumen de agrupación de almacenamiento primaria y los datos se han grabado directamente en este volumen cuando el cliente almacenó los datos, es probable que no exista ninguna copia dañada de los datos en el servidor. Si es posible, vuelva a realizar la copia de seguridad de los archivos desde el cliente.
   - Si esta agrupación de almacenamiento es un volumen de agrupación de almacenamiento primario pero los mandatos **MIGRATION**, **MOVE DATA** o **MOVE NODEDATA** colocaron los datos en este volumen, es probable que exista una copia no dañada del archivo en el servidor. Si la copia de seguridad de la agrupación de almacenamiento primaria que contenía este archivo se ha realizado en una agrupación de almacenamiento de copia antes de la ejecución de los mandatos **MIGRATION**, **MOVE DATA** o **MOVE NODEDATA**, puede que exista un archivo no dañado. Si existe un archivo no dañado, emita el mandato **UPDATE VOLUME** *nombre_volumen* **ACCESS=DESTROYED** y, a continuación, emita el mandato **RESTORE VOLUME** *nombre_volumen* para recuperar los archivos dañados para este volumen desde la agrupación de almacenamiento de copia.

Análisis de los mensajes de error ANR1330E y ANR1331E

Quizá reciba un mensaje de error ANR1330E o ANR1331E cuando se estén leyendo datos desde un volumen de agrupación de almacenamiento de IBM Spectrum Protect.

Cuando el servidor almacena datos en un volumen de agrupación de almacenamiento, de manera periódica se inserta información de auto-descripción en los datos. La validez de dicha información se comprueba mientras el servidor lee los datos. Si la comprobación indica que la información no es válida, se emiten los mensajes ANR1330E y ANR1331E. El mensaje de error ANR1330E muestra los valores reales leídos y el mensaje de error ANR1331E indica los valores esperados. El servidor emite estos mensajes por las siguientes razones:

- El hardware (subsistema de disco, unidad de cintas) ha detectado un problema al leer los datos.
- Se ha producido un error al grabar los datos y estos se han dañado.
- Se ha realizado una operación de restauración de base de datos y un volumen no se auditó adecuadamente, por lo que está en sincronización con el tiempo de restauración del punto en el tiempo (PIT).

En primer lugar debe determinar si los datos se han dañado en el soporte o si se produjo un error cuando el servidor leía los datos intactos. Emita el siguiente mandato para el volumen en el que se almacenan los datos:

```
AUDIT VOLUME FIX=NO
```

Si el informe indica que no existen archivos dañados, IBM Spectrum Protect leerá los datos anteriormente descritos como dañados correctamente. En este caso, el error se produjo por un funcionamiento incorrecto temporal del hardware mientras

el servidor leía los datos. No obstante, si el informe sigue indicando que los datos están dañados, debe determinar la causa del problema.

Puede pasar por alto el error, pero sólo si se produce con poca frecuencia. El hardware en ocasiones detecta errores al leer los datos. En la mayoría de los casos, el hardware reconoce que se ha producido un error y se recupera sin necesidad de realizar un informe sobre el mismo. Pero existen ocasiones en las que los datos se leen en un estado alterado (dañado) debido a un error temporal de hardware. En la siguiente lista se definen los resultados de la lectura de datos y recepción de un error:

Informe OK, error al leer los datos intactos en el soporte

IBM Spectrum Protect comprueba la información de auto-descripción e indica que los datos están dañados si no existen coincidencias con lo esperado. En los mensajes ANR1330E y ANR1331E, los datos aparecen como dañados.

Si tras auditar el volumen, los mensajes ANR1330E y ANR1331E se muestran con frecuencia, determine qué dispositivo de hardware provoca que los datos se lean de manera incorrecta. Consulte el registro de actividad para conocer la fecha y hora a las que se emitieron los mensajes ANR1330E y ANR1331E y facilite la información a su equipo de soporte de hardware. Con dicha información, podrán examinar los registros de error del hardware y obtener detalles sobre las operaciones que podrían haberse completado de manera anómala. Además, haga que su equipo de soporte se asegure de que el mantenimiento de los controladores de dispositivo y microcódigos esté actualizado.

Dichos errores se producen con frecuencia en las redes de área de almacenamiento (SAN). Normalmente, estos errores se presentan si se producen diversos errores de interrupción del nivel de enlace (LLI) en el conmutador o la red. Los errores de LLI indican que el sistema funciona con dificultad y provocan la modificación de datos durante la retransmisión. Solicite a su equipo de soporte de hardware que examine los registros de error de la red en busca de errores de LLI. Busque los errores de LLI registrados alrededor de la hora en que se emitieron los mensajes ANR1330E y ANR1331E.

Informe fallido, datos dañados en el soporte

Si el informe indica que los datos están dañados, se podría haber producido un error que haya provocado que los datos no se graben correctamente en el soporte. Igualmente, una operación de restauración de base de datos puede tener un volumen que no se ha auditado adecuadamente para sincronizar con el tiempo de restauración de PIT. Determine, a partir de los informes, cuándo se han grabado los datos y examine el mensaje ANR1331E para saber qué dispositivo de hardware ha dañado dichos datos. Observe los siguientes datos de ejemplo:

```
ANR1330E
The server has detected possible corruption in an object being restored
or moved. The actual values for the incorrect frame are: magic C6A2D75D
hdr version 35134 hdr length 43170 sequence number 160421181 data length
7E53DCD8 server id 348145193 segment id 327643666840426461 crc 06E04914.

ANR1331E
Invalid frame detected. Expected magic 53454652 sequence number
00000023 server id 00000000 segment id 2062.
```

El segmento ID number en el mensaje ANR1331E de este ejemplo es 2062. Para determinar la fecha en que se insertaron los datos en el servidor, emita el siguiente mandato:

```
SHOW INVO 0 2062
```

El siguiente ejemplo muestra el resultado del mandato **SHOW INVO**:

```
OBJECT: 0.2062 (Backup):
Node: NODE1 Filespace: \\node1\c$ (Unicode).
\5400\BF\ BFDEFS.H
Type: 2 (File) CG: 1 Size: 0.89088 HeaderSize: 364

BACKUP OBJECTS ENTRY:
State: 1 Type: 2 MC: 1 CG: 1
\\node1\c$ (Unicode) : \TESTFILES\ FILE1.TXT (MC: DEFAULT)
Active, Inserted 11/29/2009 13:28:26
EXPIRING OBJECTS ENTRY:
Expiring object entry not found.
```

Busque el campo `Inserted` y anote la fecha y la hora. En este ejemplo, el objeto se insertó el 11/29/2009 a las 13:28:26. Proporcione la fecha y la hora a su equipo de soporte de hardware. El equipo de soporte de hardware podrá examinar los registros de error del hardware y obtener detalles sobre las operaciones que podrían haberse completado de manera anómala. Además, pida al equipo de soporte que se asegure de que el mantenimiento de los controladores de dispositivo y microcódigos esté actualizado. Su equipo de soporte de hardware debe examinar los registros de error de la red SAN. Busque errores alrededor de la hora en la que se insertaron los datos en IBM Spectrum Protect.

Si el mandato **SHOW INVO** le facilita un resultado poco útil, emita el siguiente mandato para determinar la fecha de inserción:

```
SHOW BFO 0 xxx
```

donde xxx es el segmento ID de grupo. El siguiente ejemplo muestra el resultado del mandato **SHOW BFO**:

```
Bitfile Object: 0.xxx
**Super-bitfile 0.xxx contains following aggregated bitfiles
(offset/length)
0.2063 0.75295 0.3071 Active
0.2064 0.78366 0.88780 Active
0.2065 0.167146 0.13831 Active
0.2066 0.180977 0.21254 Active
0.2067 0.202231 0.3808 Active
0.2068 0.206039 0.11261 Active

**Disk Bitfile Entry
Bitfile Type: PRIMARY
Storage Format: 22
Logical Size: 0.217364
Physical Size: 0.221184
Number of Segments: 1,
Deleted: False
Storage Pool ID: 1
Volume ID: 2
Volume name: TapeVol1
```

Obtenga un número de archivo de bits agregado de la primera entrada de la lista de archivos de bits agregados. En el ejemplo anterior, el primer número de archivo de bits agregado es 2063. Emita el mandato **SHOW INVO** con 2063.

No existen errores de hardware en el momento de la inserción

Si el equipo de soporte de hardware no localiza errores de hardware que se produjeran a la hora de la inserción de los datos en IBM Spectrum Protect, póngase en contacto con el equipo de soporte de IBM. Proporcione al equipo el registro de actividad de la hora en que se emitieron los mensajes ANR1330E y ANR1331E. Emita también el mandato **AUDIT VOLUME FIX=NO** con el siguiente rastreo y facilite al equipo de soporte de IBM Spectrum Protect dicho rastreo:

```
TRACE ENABLE BF AF DF SS AS DS SSFRAME
TRACE DISABLE BFLOCK AFLOCK SSLOCK
TRACE BEGIN filename
```

Arreglo de archivos dañados en el soporte

Si descubre que los datos se han dañado en un volumen, emita el mandato **AUDIT VOLUME FIX=YES** en el volumen. Si las siguientes condiciones son verdaderas, los datos seguirán marcados como dañados en el volumen de agrupación primario:

- El volumen es un volumen de agrupación primario
- Se realiza una copia de seguridad de los datos en una agrupación de almacenamiento de copias
- Los datos están dañados

Una vez que se complete el mandato **AUDIT VOLUME FIX=YES**, emita el mandato **RESTORE VOLUME** para el volumen de agrupación primario. Los datos dañados se sustituyen por una nueva copia de los mismos. Si el mandato **AUDIT VOLUME FIX=YES** lee los datos correctamente, los datos dejarán de indicarse como dañados en la agrupación de almacenamiento primario.

Si no existe una copia de seguridad, el mandato **AUDIT VOLUME FIX=YES** eliminará los datos. Si los datos eliminados son una copia de seguridad, estos se ubicarán en el servidor la próxima vez que se ejecute la copia de seguridad del cliente.

Si los datos que están siendo eliminados por el mandato **AUDIT VOLUME FIX=YES** se encuentran en un volumen de agrupación de almacenamiento de copias, estos se eliminarán del volumen de agrupación de copias. La próxima vez que se realice una copia de seguridad de la agrupación de almacenamiento primario, se añadirá una nueva copia a la agrupación de almacenamiento de copias.

No se da caducidad a los archivos después de reducir las versiones

Puede actualizar las políticas del servidor para reducir el número de versiones de un archivo que desea conservar, sin embargo, se pueden generar errores debido a estas actualizaciones en algunas ocasiones.

Emita el mandato **QUERY COPYGROUP** *nombre_dominio nombre_conjunto_políticas nombre_grupo_copia* **F=D**. Si se han cambiado los parámetros **Versiones si datos existen** o **Versiones si datos suprimidos** para un grupo de copia **TYPE=BACKUP** es posible que esto afecte a la caducidad.

Si se han reducido los valores **Versiones si datos existen** o **Versiones si datos suprimidos** para un grupo de copia **TYPE=BACKUP**, es posible que el proceso de caducidad del servidor no lo reconozca inmediatamente y estos archivos caduquen. El servidor sólo aplica los valores de **Versiones si datos existen** y **Versiones si datos suprimidos** a los archivos en el momento en que se realiza la copia de

seguridad de los mismos en el servidor. Cuando se realiza la copia de seguridad de un archivo, el servidor contabiliza el número de versiones de dicho archivo y, si éste excede el número de versiones que deben conservarse, el servidor marca las versiones más antiguas que exceden este valor para caducidad.

Síntomas de proceso que indican errores de migración

Es posible que se enfrente con síntomas de proceso que señalen a una migración como la causa de los errores.

La migración no se ejecuta para una agrupación de almacenamiento de medios secuenciales

Si la migración no se ejecuta para las agrupaciones de almacenamiento de soportes secuenciales, emita el mandato **QUERY STGPOOL** *stgpoolName* **F=D**.

La migración desde las agrupaciones de almacenamiento de medios secuenciales calcula el valor de "Pct. Util" como el número de volúmenes que están utilizándose para la agrupación de almacenamiento en relación con el número total de volúmenes que pueden utilizarse para esa agrupación de almacenamiento. De forma similar, calcula el valor de "Pct. Migr" como el número de volúmenes con datos, que pueden migrarse, que están utilizándose para la agrupación de almacenamiento, en relación con el número total de volúmenes que pueden utilizarse para esa agrupación de almacenamiento. Puesto que en este cálculo podrían considerarse los volúmenes reutilizables, puede que parezca que no existen datos suficientes que puedan migrarse en la agrupación de almacenamiento como para que sea necesario un proceso de migración.

La migración sólo utiliza un proceso

Emita el mandato **QUERY STGPOOL** *nombre_agrupación_almacenamiento* **F=D** y **QUERY OCCUPANCY * * STGPOOL**= *nombre_agrupación_almacenamiento*.

Los siguientes son los motivos por qué se ejecuta sólo un proceso de migración:

- El valor de procesos de migración para la agrupación de almacenamiento se ha establecido en uno o no se ha definido (está en blanco). Si es así, emita el mandato **UPDATE STGPOOL** *nombre_agrupación_almacenamiento* **MIGPROCESS**=*n*, donde *n* es el número de procesos que se van a utilizar para migrar desde esta agrupación. Tenga en cuenta que este valor debe ser menor que o igual al número de unidades (límite de montaje) para la SIGUIENTE agrupación de almacenamiento en la que la migración está almacenando datos.
- Si el mandato **QUERY OCCUPANCY** sólo notifica un único nodo cliente y un espacio de archivos en esta agrupación de almacenamiento, la migración sólo se puede ejecutar un único proceso si el valor Procesos migración para la agrupación de almacenamiento es superior a uno. El proceso de migración particiona datos, en función del nodo cliente y del espacio de archivos. Para que la migración pueda ejecutarse con varios procesos, en esa agrupación de almacenamiento deben estar disponibles los datos para más de un nodo cliente.

Resolución de problemas de agrupación de almacenamiento

Las agrupaciones de almacenamiento son un parte esencial para el funcionamiento correcto del servidor. La base de datos de IBM Spectrum Protect contiene información en agrupaciones de almacenamiento sobre nodos cliente inscritos, políticas y planificaciones, así como información sobre los datos del cliente.

Esta información debe estar disponible y ser válida para que IBM Spectrum Protect funcione correctamente. Los errores de las agrupaciones de almacenamiento pueden estar relacionados con los siguientes problemas:

- Transacciones con anomalías
- Una agrupación de almacenamiento que experimenta un alto volumen de utilización después de haberse incrementado el valor de MAXSCRATCH
- Una agrupación de almacenamiento que tiene "Collocate?=Yes", pero los volúmenes siguen conteniendo datos para muchos nodos
- No pueden almacenarse datos en una agrupación de datos activos utilizando la grabación simultánea o emitiendo el mandato **COPY ACTIVEDATA**

Se ha recibido el mensaje "ANR0522W Ha fallado la transacción..."

El mensaje ANR0522W se visualiza cuando el servidor no pueden asignar espacio en la agrupación de almacenamiento que se ha identificado para almacenar datos para el cliente especificado.

Acerca de esta tarea

La insuficiencia de espacio en una agrupación de almacenamiento puede deberse a varias causas posibles. Realice lo siguiente para resolver el error de asignación de espacio:

Procedimiento

1. Emita **QUERY VOLUME** *nombrevol* **F=D** para los volúmenes en la agrupación de almacenamiento referenciada. Si se informa de la existencia de algún volumen con un acceso distinto del acceso de lectura/grabación, compruebe ese volumen. Puede que un volumen se haya marcado como volumen de sólo lectura o como no disponible a causa de un error de dispositivo. Si se ha resuelto el error del dispositivo, emita el mandato **UPDATE VOLUME** *nombrevol* **ACCESS=READWRITE** para permitir que el servidor seleccione e intente grabar datos en dicho volumen.
2. Emita **QUERY VOLUME** *nombrevol* para los volúmenes en la agrupación de almacenamiento referenciada. Los volúmenes que tienen el estado de volumen "pendiente" son volúmenes que están vacíos pero a la espera de que el servidor vuelva a utilizarlos. El tiempo de espera está controlado por el valor REUSEDELAY de la agrupación de almacenamiento y se visualiza como "Período de retardo de la reutilización de un volumen" en el mandato **QUERY STGPOOL**. Evalúe el valor REUSEDELAY para esta agrupación de almacenamiento y, si procede (basándose en los criterios de gestión de datos), disminuya este valor emitiendo el mandato **UPDATE STGPOOL** *nombre_agrupación_almacenamiento* **REUSEDELAY**=*nn*, donde *nombre_agrupación_almacenamiento* es el nombre de la agrupación de almacenamiento y *nn* es el nuevo valor de retardo de la reutilización. La clave para que exista proximidad de datos consiste en disponer de espacio suficiente en la agrupación de almacenamiento de destino para que el proceso de proximidad seleccione un volumen adecuado. El número de volúmenes

reutilizables de una agrupación de almacenamiento afecta de forma significativa a la existencia de espacio suficiente en la agrupación de almacenamiento de destino.

3. Emita el mandato **QUERY STGPOOL F=D** para verificar si el ACCESS es de lectura/grabación.

La agrupación de almacenamiento experimenta un alto volumen de utilización después de haberse incrementado el valor de MAXSCRATCH

Para agrupaciones de almacenamiento secuenciales de proximidad, incrementar el valor **MAXSCRATCH** puede hacer que el servidor utilice más volúmenes.

El servidor utiliza más volúmenes de agrupación de almacenamiento en este caso debido al proceso de proximidad. La proximidad agrupa los datos de usuario para un nodo cliente en la misma cinta. Durante una operación de copia de seguridad o archivado de cliente, si actualmente ninguna cinta tiene datos para este nodo cliente, el servidor selecciona un volumen reutilizable para almacenar los datos. A continuación, para otros nodos cliente que almacenan datos, el servidor selecciona de nuevo un volumen reutilizable. El motivo por el que no se seleccionan volúmenes reutilizables antes de cambiar el valor **MAXSCRATCH** es que si no hay ningún volumen reutilizable disponible y ningún volumen preferido ya asignado para este nodo de cliente, el proceso de selección de volumen en el servidor ignora la petición de proximidad y almacena los datos en un volumen disponible.

La agrupación de almacenamiento se establece para utilizar la asignación, pero los volúmenes contienen datos que no están asignados

Cuando una agrupación de almacenamiento está habilitada para la asignación (el parámetro **COLLOCATION** está establecido en GROUP, NODE o FILESPACE), es posible que muchos volúmenes contengan datos que no estén asignados.

Existen dos posibilidades para esta situación:

- Los datos se ha almacenado en volúmenes de esta agrupación de almacenamiento antes de habilitar la agrupación de almacenamiento para la asignación.
- La agrupación de almacenamiento no disponía de suficientes cintas reutilizables y ha almacenado los datos en el mejor volumen posible, aunque ha pasado por alto la petición de proximidad.

Si los datos para múltiples nodos finalizan en el mismo volumen para una agrupación de almacenamiento que está habilitada para la asignación, utilice una de las siguientes acciones:

- Emita el mandato **MOVE DATA** para el volumen o volúmenes afectados. El proceso lee los datos del volumen especificado y los mueve a un volumen diferente de la misma agrupación de almacenamiento si:
  - Si hay disponibles volúmenes reutilizables o
  - Si se asignan volúmenes con suficiente espacio a este nodo de cliente para asignar los datos
- Permita que la migración traspase todos los datos desde esa agrupación de almacenamiento estableciendo los umbrales HIGHMIG y LOWMIG. Si se

permite la migración de todos los datos a la SIGUIENTE agrupación de almacenamiento, los requisitos de asignación se procesan si se cumple lo siguiente:
  - La SIGUIENTE agrupación de almacenamiento está habilitada para la asignación
  - La SIGUIENTE agrupación de almacenamiento tiene suficientes volúmenes reutilizables
  - A la SIGUIENTE agrupación de almacenamiento se le asignan volúmenes para satisfacer los requisitos de asignación
- Emita el mandato **MOVE NODEDATA** para los nodos de cliente cuyos datos están en esa agrupación de almacenamiento. Si hay volúmenes reutilizables disponibles o si a este nodo de cliente se le asignan volúmenes con suficiente espacio para asignar los datos, se producen los sucesos siguientes:
  - El proceso **MOVE NODEDATA** lee los datos de los volúmenes en los que este nodo tiene datos
  - El proceso **MOVE NODEDATA** mueve datos a un volumen o a volúmenes diferentes de la misma agrupación de almacenamiento

La clave para que exista proximidad de datos consiste en disponer de espacio suficiente en la agrupación de almacenamiento de destino para que el proceso de proximidad seleccione un volumen adecuado. Debe haber suficientes volúmenes vacíos disponibles en la agrupación de almacenamiento para permitir que la asignación seleccione un nuevo volumen. Asegúrese de que hay suficientes volúmenes vacíos disponibles en lugar de un volumen que ya tiene datos de un nodo diferente. Los volúmenes vacíos pueden ser volúmenes reutilizables si la agrupación de almacenamiento se define con suficientes volúmenes reutilizables o defina los volúmenes vacíos emitiendo el mandato **DEFINE VOLUME**.

Resolución de problemas de almacenamiento para agrupaciones de datos activas

Es posible que experimente dificultades al almacenar datos en una agrupación de datos activa utilizando la función de grabación simultánea o emitiendo el mandato **COPY ACTIVEDATA**.

Para que los datos puedan almacenarse en una agrupación de datos activos, debe establecer una política que permita la colocación de los datos en la agrupación. El nodo que es el propietario de los datos debe asignarse a un dominio cuya agrupación de datos activos se indique en el campo ACTIVEDESTINATION del dominio. Emita el mandato siguiente para determinar si el nodo se ha asignado a un dominio que autoriza el almacenamiento en la agrupación de datos activa:

```
QUERY NODE  nombre_nodo F=D
```

En el campo Nombre de dominio de políticas se indica el dominio al que se ha asignado el nodo. Emita el mandato siguiente para determinar si la agrupación de datos activa está listada en el campo ACTIVEDESTINATION del dominio:

```
QUERY DOMAIN nombre_dominio F=D
```

Si la agrupación de datos activos no está listada, emita el siguiente mandato para añadir la agrupación de datos activos a la lista:

```
UPDATE DOMAIN nombre_dominio ACTIVEDESTINATION=nombre_agrupación_datos-activa
```

Consejo: Tras emitir el mandato **UPDATE DOMAIN** *nombre_dominio* **ACTIVEDESTINATION**=*nombre_agrupación_datos_activos*, todos los nodos asignados al

dominio tienen autorización para almacenar datos en la agrupación de datos activos. Si no es aceptable tener los nodos asignados al dominio autorizados para almacenar datos, deberá crear un nuevo dominio para los nodos cuyos datos desea que se almacenen en la agrupación de datos activos y deberá asignar esos nodos al dominio que acaba de crearse.

Resolución de problemas con agrupaciones de almacenamiento de contenedor en la nube

Con IBM Spectrum Protect, puede realizar una copia de seguridad de los datos y restaurarlos directamente desde una agrupación de almacenamiento de contenedor en la nube.

Es posible que detecte problemas de rendimiento o limitaciones con las agrupaciones de almacenamiento de contenedor en la nube. Para obtener información adicional, consulte las preguntas más frecuentes para las agrupaciones de almacenamiento de contenedor en la nube en IBM developerWorks.

Utilice las instrucciones siguientes para resolver problemas y gestionar limitaciones:

Problemas con la supresión de objetos de la nube
El rendimiento de una agrupación de almacenamiento de contenedor en la nube depende de la conexión de red entre el servidor y la nube. En función del proveedor de la nube, la supresión de objetos del almacenamiento en la nube puede tardar bastante tiempo. Por ejemplo, si utiliza Swift OpenStack como proveedor de la nube, debe suprimir los objetos de la nube de forma individual, y la latencia de la red afecta a cada operación de supresión. Si tiene que suprimir muchos objetos de la nube en poco tiempo, asegúrese de que IBM Spectrum Protect pueda suprimir todos los objetos guardados en la nube. Por ejemplo, es posible que el rendimiento sea bajo si utiliza un proveedor de nube local y suprime con regularidad grandes espacios de archivos de IBM Spectrum Protect.

Eliminación de datos marcados como dañados o huérfanos durante una auditoría
Una extensión de datos dañada es un archivo que tiene referencias en la base de datos del servidor, pero a la que le faltan datos, o que contiene datos dañados, en la nube. Una extensión de datos huérfanos es un objeto almacenado en un proveedor de servicios en la nube que no tiene ninguna referencia en la base de datos de servidor. El parámetro **FORCEORPHANDBDELETE** del mandato **AUDIT CONTAINER** permite al servidor forzar la eliminación de las extensiones huérfanas de la base de datos del servidor, aunque no se eliminen de la agrupación de almacenamiento de contenedores en la nube. Este parámetro es opcional.

Problemas de rendimiento con la restauración de archivos
Si detecta un bajo rendimiento al restaurar archivos, compruebe que la operación de restauración esté disponible en su entorno. Consulte la nota técnica 1659833.

Restricciones para las agrupaciones de almacenamiento de contenedor en la nube Las siguientes funciones no son compatibles con las agrupaciones de almacenamiento de contenedor en la nube:

- Réplica de una agrupación de almacenamiento de contenedor en la nube con el mandato **PROTECT STGPOOL**
- Migración

- Reclamación
- Agregación
- Asignación
- Operaciones de grabación simultánea
- Operaciones de copia de agrupación de almacenamiento
- Uso de volúmenes virtuales

Además, no puede utilizar el parámetro **NEXTSTGPOOL** con el mandato **DEFINE STGPOOL** en una agrupación de almacenamiento de contenedor en la nube ni con una agrupación de almacenamiento de contenedor en directorio porque IBM Spectrum Protect no puede determinar cuándo se llena el proveedor de almacenamiento en la nube. Utilice el parámetro **NEXTSTGPOOL** para especificar únicamente una agrupación de almacenamiento de acceso aleatorio o secuencial primario. Como resultado, la capacidad de desbordamiento no está disponible para las agrupaciones de almacenamiento basado en contenedor.

No se puede realizar una recuperación de error en la nube cuando el almacenamiento local está lleno

Si utiliza directorios de la agrupación de almacenamiento con una agrupación de almacenamiento de contenedor en la nube y no queda espacio libre en los directorios, las operaciones de seguridad se detienen de forma prematura. Para evitar esta situación, asigne más directorios de la agrupación de almacenamiento para ofrecer más espacio de almacenamiento local a la agrupación de almacenamiento para operaciones de copia de seguridad. También puede esperar a que los datos se limpien automáticamente de los directorios locales después de mover los datos a la nube.

Limitaciones en el uso de la réplica de nodo con una agrupación de almacenamiento de contenedor en la nube

Puede utilizar una agrupación de almacenamiento de contenedor en la nube como agrupación de almacenamiento de destino en un servidor de réplica de destino. Sin embargo, no puede utilizar una agrupación de almacenamiento de contenedor en la nube como agrupación de almacenamiento de destino en un servidor de réplica de origen. Para proporcionar la función de redundancia, utilice las funciones de réplica disponibles en el proveedor de almacenamiento en la nube.

Tipos de archivo que se deben evitar con agrupaciones de almacenamiento de contenedor en la nube

Para una agrupación de almacenamiento de contenedor en la nube, evite el almacenamiento de tipos de datos de cliente que no estén optimizados para almacenar datos en agrupaciones de almacenamiento de soporte extraíble. Por ejemplo, evite almacenar archivos de control de VMware y archivos de metadatos de Data Protection for SQL (para copias de seguridad de SQL heredadas). Para obtener más información, consulte los siguientes documentos:

- Uso de cintas, bibliotecas VTL o agrupaciones de almacenamiento de contenedores con IBM Spectrum Protect for Virtual Environments, nota técnica 1659833
- IT11763: FALTAN LAS CONSIDERACIONES SOBRE METADATOS EN LA DOCUMENTACIÓN DE DATA PROTECTION FOR SQL SERVER.

Capítulo 4. Resolución de problemas del centro de operaciones

AIX Linux Windows

Si se produce un problema con el Centro de operaciones de IBM Spectrum Protect y no puede resolverlo, puede consultar las descripciones de problemas conocidos para encontrar una posible solución. Es posible que también tenga que revisar los archivos de registro y habilitar el rastreo ampliado para Operations Center.

Visión general de los archivos de registro

AIX Linux Windows

Si ha contactado con el servicio de soporte de software de IBM acerca de un problema con el Operations Center, es posible que se le solicite que envíe los archivos de registro.

Lista de los archivos de registro

Es posible que el servicio de soporte de software de IBM le solicite que envíe los archivos de registro siguientes:

- Hasta ocho archivos de registro del Operations Center:
  - `tsm_opscntr.log`
  - `tsm_opscntr1.log`
  - `tsm_opscntr2.log`
  - `tsm_opscntr3.log`
  - `tsm_opscntr4.log`
  - `tsm_opscntr5.log`
  - `tsm_opscntr6.log`
  - `tsm_opscntr7.log`

  Pueden existir más de un archivo de registro del Operations Center por los motivos siguientes:
  - Si el registro del Operations Center tiene más de 8 MB, la versión actual es `tsm_opscntr.log`, la versión anterior es `tsm_opscntr1.log`, la versión anterior a esta es `tsm_opscntr2.log`, etc.
  - Si el registro del Operations Center tiene un tamaño superior a los 8 MB, el registro se distribuye en varios archivos, cada uno con un tamaño máximo de 8 MB. Por ejemplo, si el registro tiene un tamaño de 15 MB, se distribuye en los archivos `tsm_opscntr.log` y `tsm_opscntr1.log`.

  Consejo: Si el servicio de soporte de software de IBM le solicita que realice un rastreo ampliado del Operations Center, puede identificar los archivos de registro del Operations Center que se han creado durante el rastreo mediante las horas de modificación de los archivos.
- Archivos de registro del servidor web:
  - `console.log`
  - `messages.log`

- Archivos FFDC (First-failure-data-capture):
  - `resumen_excepción_`*`fecha_hora`*`.log`
  - `ffdc_`*`fecha_hora`*`.log`

Ubicación de los archivos de registro

- Los archivos de registro del Operations Center y del servidor web están en el directorio siguiente:

  AIX Linux *`installation_dir`*`/ui/Liberty/usr/servers/guiServer/logs`

  Windows *`installation_dir`*`\ui\Liberty\usr\servers\guiServer\logs`

  donde *`installation_dir`* es el directorio en el que está instalado IBM Spectrum Protect. Por ejemplo:

  AIX Linux `/opt/tivoli/tsm`

  Windows `c:\Program Files\Tivoli\TSM`

  Consejo: También puede ver el registro del Operations Center desde el Operations Center.
- Los archivos de registro FFDC están en la misma ubicación pero en el subdirectorio `ffdc`.

Tareas relacionadas:

"Inicio de un rastreo ampliado del Centro de operaciones" en la página 123

Visualización del registro del Centro de operaciones en el Centro de operaciones

AIX Linux Windows

El registro del Operations Center contiene datos de rastreo de los sucesos del Operations Center. Puede ver el registro en el Operations Center o puede ir al directorio que contiene el archivo de registro y abrir el archivo.

Procedimiento

Para ver el registro del Operations Center cuando ha iniciado la sesión en el Operations Center, siga estos pasos:

1. En la barra de menús del Operations Center, pase el puntero sobre el icono de signo de interrogación y seleccione **Acerca del Centro de operaciones**.
2. En la ventana que se muestra, pulse **Detalles de la instalación**.
3. Pulse el separador **Ver registro**.
4. Pulse **Visualizar registro**.

Tareas relacionadas:

"Inicio de un rastreo ampliado del Centro de operaciones" en la página 123

No se han actualizado las alertas inmediatamente

AIX Linux Windows

En la página de Alertas del Operations Center, cuando intenta asignar varias alertas a un administrador o cerrar varias alertas, dichas alertas no se asignan o cierran de forma inmediata.

Síntoma

Tabla 8 muestra datos de ejemplo de un entorno de pruebas cuando un administrador ha actualizado varias alertas. Los resultados pueden diferir de los resultados en el entorno de almacenamiento.

Tabla 8. Los tiempos de retardo aproximado de las alertas se actualizaron en un entorno controlado

Cantidad de alertas actualizadas	Retardo para las alertas del servidor hub	Retardo de las alertas desde los servidores de radio con IBM Spectrum Protect Versión 7.1.0	Retardo de las alertas desde los servidores spoke con V6.3.4
1	6 segundos	7 segundos	7 segundos
10	6 segundos	7 segundos	9 segundos
100	6 segundos	8 segundos	40 segundos
1 000	10 segundos	20 segundos	5,5 minutos
10 000	45 segundos	1,25 minutos	1 hora

Por ejemplo, cuando un administrador selecciona 10 000 alertas de servidor hub y hace clic en **Close** (cerrar), se tarda aproximadamente 45 segundos en cerrar las alertas.

Solución

Espere hasta que la alerta se actualiza o actualice el número de alertas una por una. Para obtener tasas de respuesta más rápidas, actualice los servidores spoke que ejecuten V6.3.4 a V7.1 o posterior.

Las tareas activas no se cancelan inmediatamente

AIX Linux Windows

Cuando selecciona varias tareas en la página Active Tasks (Tareas activas) del Operations Center e intenta cancelarlas, las tareas no se cancelan inmediatamente. Existe un retardo más largo para las tareas del servidor spoke que para las tareas del servidor hub.

Síntoma

Tabla 9 en la página 110 muestra datos de ejemplo de un entorno de pruebas cuando un administrador ha cancelado variastareas. Los resultados pueden diferir de los resultados en el entorno de almacenamiento.

Tabla 9. Tiempos de retardo aproximados cuando se cancelan las tareas en un entorno controlado

Número de tareas canceladas	Retardo de las tareas del servidor hub	Retardo de las tareas del servidor spoke
1	5 segundos	5 segundos
10	5 segundos	7 segundos
100	10 segundos	25 segundos.
1000	40 segundos	3,5 minutos

Por ejemplo, cuando un administrador ha seleccionado 1000 tareas de servidor hub y ha pulsado en **Cancel** (Cancelar), se tardan aproximadamente 40 segundos para que las tareas se cancelaran.

Solución

Espere hasta que la tarea se ha cancelado y cancele las tareas una por una.

Problemas conocidos del Centro de operaciones

AIX Linux Windows

Los problemas conocidos se documentan en forma de notas técnicas en la base de datos de conocimientos de soporte. IBM Software Support actualiza la bases de datos de conocimientos a medida que se detectan y resuelven problemas. Puede encontrar rápidamente soluciones a los problemas buscando en la base de conocimientos.

- Para obtener una lista de problemas conocidos, consulte la página web siguiente en la base de conocimiento de soporte: Problemas conocidos del Centro de operaciones de IBM Spectrum Protect.
- Para ver otros problemas que se han conocido después del lanzamiento del producto, consulte los siguientes resultados de búsqueda: Resultados de búsqueda de problemas conocidos con Centro de operaciones de IBM Spectrum Protect.

Capítulo 5. Resolución de problemas de comunicación

La necesidad de conectividad en IBM Spectrum Protect significa que cualquier error en las comunicaciones podría hacer que la aplicación dejara de funcionar. Los errores de comunicación pueden deberse a la configuración TCP/IP, a las conexiones del cliente y del servidor y a otras causas.

Resolución de problemas originados al conectarse al servidor

Los problemas generados al conectarse con el servidor podrían estar relacionados con las opciones de comunicación.

Para corregir el error, realice alguna o todas las acciones siguientes:

- Revise los cambios en las opciones de comunicación de cliente del archivo de opciones de cliente (si se ha realizado alguno) e intente volver a los valores anteriores. Vuelva a intentar conectarse.
- Si se han cambiado los valores de comunicación de servidor, actualice las opciones de comunicación de cliente de modo que reflejen los valores de servidor modificados, o bien devuelva al servidor los valores anteriores.
- Si se han cambiado los valores de red, como la dirección TCP/IP del cliente o del servidor (o un cortafuegos), trabaje con el administrador de la red para actualizar el cliente, el servidor o ambos para estos cambios en la red.

Resolución de conexiones anómalas por parte de clientes o administradores

Las dos principales causas de las anomalías de conexión son una anomalía general, en la que no es posible establecer ninguna conexión o una anomalía aislada, en la que es posible establecer algunas conexiones, pero no otras.

Si no es posible establecer ninguna conexión, puede que sea necesario ejecutar el servidor en primer plano para que exista una consola de servidor disponible y puedan realizarse pasos de diagnóstico adicionales. Compruebe los valores para verificar la correcta configuración para la comunicación con el servidor:

- Asegúrese de que el servidor pueda vincularse a un puerto al iniciarse. Si no puede vincularse a un puerto, es probable que otra aplicación esté utilizando ese puerto. El servidor no puede vincularse (utilizar) a un puerto TCP/IP determinado si otra aplicación ya se ha vinculado a ese puerto. Si el servidor se ha configurado para las comunicaciones TCP/IP y se vincula correctamente a un puerto al tener lugar el inicio de sesión para las sesiones cliente, se emite el mensaje siguiente:

  ```
  ANR8200I Controlador de TCP/IP listo para la conexión con clientes
  en puerto 1500.
  ```

  Si se ha configurado un método de comunicación determinado en el archivo de opciones del servidor, pero no se envía un mensaje de vinculación correcta durante el inicio del servidor, existe un problema en la inicialización para ese método de comunicación.
- Compruebe que el valor de **TCPPORT** del código del archivo de opciones del servidor sea correcto. Si se cambia por equivocación el valor del código, los

clientes no podrán conectarse. Esto se debe a que los clientes intentarán conectarse con un puerto TCP/IP distinto del puerto en el que el servidor está a la escucha.

- Si varios servidores utilizan la misma dirección TCP/IP, asegúrese de que los valores de **TCPPORT** y **TCPADMINPORT** de cada servidor son exclusivos. Por ejemplo, existen dos servidores en la misma dirección TCP/IP. El primer servidor tiene un valor de **TCPPORT** de 1500 y un valor de **TCPADMINPORT** de 1500. El segundo servidor tiene un valor de **TCPPORT** de 1501 y un valor de **TCPADMINPORT** que es 1500. El primer servidor que obtiene el puerto 1500 bloquea el acceso del otro servidor al puerto 1500 y los clientes ya no pueden acceder al primer servidor. Los clientes de administración siempre se conectan con el segundo puerto. Una mejor opción para los puertos de cada servidor sería 1500 y 1501 para TCPPORT y 1510 y 1511 para **TCPADMINPORT**.
- Compruebe que el servidor se ha activado para las sesiones. Emita el mandato **QUERY STATUS** y verifique que se haya establecido "Disponibilidad: Habilitada". Si el resultado establece "Disponibilidad: Inhabilitada," emita el mandato **ENABLE SESSIONS**.
- Si clientes específicos no pueden conectarse con el servidor, compruebe los valores de comunicación que se han establecido para esos clientes. Con TCP/IP, compruebe las opciones TCPSERVERADDRESS y **TCPSERVERPORT** en el archivo de opciones de cliente.
- Si el servidor sólo rechaza un nodo específico, verifique que el nodo no está bloqueado en el servidor. Emita el mandato **QUERY NODE** *nombre_nodo*, donde *nombre_nodo* es el nombre del nodo que hay que comprobar. Si el resultado indica "Locked?: Yes,", determine por qué está bloqueado este nodo. Los nodos sólo se pueden bloquear utilizando el mandato administrativo **LOCK NODE**. Si conviene desbloquear este nodo, emita el mandato **UNLOCK NODE** *nombre_nodo*, donde *nombre_nodo* es el nombre del nodo que hay que desbloquear.
- Si el sistema en el que se ejecuta el servidor está experimentado problemas de asignación de memoria o de recursos, puede que no sea posible iniciar nuevas conexiones con el servidor. El problema relacionado con la asignación de memoria o de recursos, puede eliminarse temporalmente si detiene y reinicia el servidor o si detiene y reinicia el propio sistema. Esta acción es una solución temporal y el diagnóstico debe continuar para el sistema operativo o para el servidor porque el problema de asignación de recursos puede indicar un error en uno de los dos.

Resolución de errores de Capa de sockets seguros

Los errores de SSL pueden deberse a una configuración incorrecta del entorno, a un certificado del servidor erróneo, a problemas de conexión, a condiciones de falta de sincronización o a otras causas.

Utilice las instrucciones siguientes para resolver problemas comunes de SSL de cliente a servidor y de servidor a servidor:

Falta de conexión al servidor tras utilizar un certificado de la entidad emisora de certificados (CA) de terceros

Si utiliza un certificado de terceros y éste no se ha añadido al servidor, especifique el certificado raíz como de confianza en la base de datos de claves del servidor. Para añadir el certificado raíz a la base de datos, emita este mandato:

```
gsk8capicmd -cert -add -db cert.kdb -pw contraseña
-label name -file .der_file -format ascii
```

El certificado raíz de CA no se ha añadido al cliente

Añada el certificado raíz como de confianza en la base de datos de claves del cliente:

```
gsk8capicmd -cert -add -db dsmcert.kdb -pw contraseña
-label my CA -file ca.arm -format ascii
```

No se puede ejecutar gsk8capicmd.exe (IBM Global Security Kit [GSKit])

En la mayoría de los casos, este error de Windows lo genera una configuración incorrecta del entorno. Configure la variable PATH como se indica antes de ejecutar el programa de utilidad gsk8capicmd.

ANS1595E Certificado de servidor erróneo

Este error se notifica cuando el certificado del servidor es desconocido para el cliente o el servidor. El error de "certificado de servidor erróneo" se puede producir en estas circunstancias:

- El certificado nunca se ha importado
- El archivo de certificados `cert256.arm` estaba dañado antes de importarlo
- El mandato para importar el certificado se ha especificado incorrectamente
- La variable *DSM_DIR* apunta al directorio erróneo, que contiene una base de datos de claves de cliente incorrecta (`dsmcert.kdb`)
- El servidor se configura para TLS (Transport Layer Security) 1.2, pero el cliente no se encuentra en un nivel suficiente (es necesario 6.3).
- El servidor se configura para TLS 1.2, pero el cliente ha importado el archivo `cert.arm` en lugar del archivo `cert256.arm`.
- El servidor se configura para TLS 1.2, pero el cliente ha importado el archivo `cert256.arm` en lugar del archivo `cert.arm`.

Repita todos los pasos necesarios para importar el certificado de servidor y compruebe la variable *DSM_DIR*. Para obtener más información acerca del error, consulte el archivo `dsmerror.log`. El registro de errores de cliente también pueden contener información sobre un error específico de IBM GSKit.

ANS1592E No se ha podido inicializar el protocolo SSL

Este error se produce en el cliente e indica que no se ha establecido la conexión SSL. Para obtener más información acerca del error, consulte el registro de errores del cliente. El servidor no acepta sesiones SSL en el puerto al que el cliente o el servidor está intentando conectarse. Determine si el cliente o el servidor apuntan al puerto del servidor correcto (TCPPort), el cual puede ser un número de puerto diferente al valor predeterminado 1500.

ANR8583E y el código de retorno GSKit 406

Este error puede indicar que un cliente que no está habilitado para SSL está intentando ponerse en contacto con un puerto SSL. Cuando un cliente establece contacto con un servidor en un puerto definido mediante `SSLTCPPORT` o `SSLTCPADMINPORT`, el servidor establece una sesión e inicia un "reconocimiento" SSL. Si el cliente no está habilitado para SSL, no puede completar el proceso de reconocimiento SSL. La sesión entonces parece detenerse, pero agotará el tiempo de espera a través de la opción `IDLEWAIT` del servidor o bien finalizará cuando el administrador del servidor emita el mandato **`CANCEL SESSION`** para cancelarla manualmente. El ejemplo muestra una sesión con este estado, desde el servidor:

```
TSM:SERVER1>query session
ANR2017I El administrador SERVER_CONSOLE ha emitido el mandato: QUERY SESSION

  Núm. Método  Estado Tiempo Bytes   Bytes  Tipo   Plataf.  Nombre cliente
sesión comun. sesión espera enviad. recib. sesión
------ ------ ------ ------ ------- ------- ----- -------- -------------
     1 SSL    IdleW   17 S        0       0 Node
```

Importante: Dado que el entorno de sistemas puede producir que un proceso de reconocimiento válido tarde algún tiempo en completarse, no presuponga que el resultado anterior indica siempre que se trata de un cliente que no es SSL.

ANR8583E y el código de retorno GSKit 420, así como ANR8581E con el código de retorno GSKit 406 se producen para la misma sesión de cliente de IBM Spectrum Protect

Cuando los mensajes del servidor ANR8583E y ANR8581E se producen para la misma sesión de cliente, es probable que el cliente haya generado un mensaje ANS1595E. El mensaje ANS1595E normalmente se emite cuando IBM Spectrum Protect intenta establecer una sesión con el servidor. En este caso, siga las instrucciones que se indican en el manual de mensajes de IBM Spectrum Protect para ANS1595E con objeto de eliminar estos errores.

ANR3338E TLS está en un nivel anterior a 1.2

Este error se notifica cuando el servidor y el agente de almacenamiento intentan conectarse con un protocolo SSL anterior a TLS 1.2. En la comunicación del servidor y el agente de almacenamiento, si se especifica la opción `SSLDISABLELEGACYTLS`, las sesiones TLS se deben conectar en un nivel mínimo de TLS 1.2 o se rechazará la sesión.

Los servidores de varias definiciones sin SSL=YES ocasionan un cuelgue del servidor

Si planea utilizar la comunicación SSL, la infraestructura SSL debe estar en su lugar en los servidores de réplica del origen y del destino. Los certificados SSL necesarios deben estar en el archivo de base de datos clave que pertenece a cada servidor. La función SSL estará activa si el archivo de opciones del servidor contiene la opción `SSLTCPPORT` o `SSLTCPADMINPORT` o si un servidor se define con **SSL=YES** en el arranque.

Si un certificado de terceros en uso no se ha añadido al servidor, o si el certificado de CA no se ha añadido al cliente, se creará una entrada. Cuando se inicia una sesión SSL, el mensaje de inicio de sesión incluye el número de serie del certificado de servidor. De esta forma, el certificado que se está utilizando se puede identificar de forma exclusiva.

Referencia relacionada:

Apéndice C, “Códigos de retorno de IBM Global Security Kit”, en la página 221

Recuperación de la contraseña del archivo de base de datos de claves

Si ha olvidado la contraseña del archivo de base de datos de clave actual, IBM Spectrum Protect puede ayudarle a recuperarla.

Antes de empezar

Para administrar la recuperación de la contraseña del archivo de base de datos de claves debe tener privilegios del sistema.

Acerca de esta tarea

Para recuperar y actualizar la contraseña del archivo de base de datos de claves, siga los pasos indicados a continuación:

Procedimiento

1. Emita el mandato **QUERY SSLKEYRINGPW** para mostrar la contraseña de la base de datos de claves actual.
2. Emita el siguiente mandato para utilizar el registro del servidor sobre la contraseña de la base de datos de claves para actualizar la contraseña:

   ```
   SET SSLKEYRINGPW password UPDATE=Y
   ```

   donde *password* es la contraseña recuperada por el mandato **QUERY SSLKEYRINGPW**.

Qué hacer a continuación

Consejo: Si el archivo `cert.kdb` no existe, podrá crear un archivo nuevo reiniciando el servidor. El servidor crea un archivo de base de datos con la contraseña antigua y genera un nuevo certificado autofirmado durante el inicio. Si utiliza certificados autofirmados, debe extraer el certificado e instalarlo en un sistema cliente. Si utiliza un certificado de terceros, debe añadirlo de nuevo al archivo de base de datos de claves del servidor y reiniciar dicho servidor.

Resolución de problemas de la base de datos de claves de certificados

Las copias de seguridad del archivo `cert.kdb` garantizan que TLS (Transport Layer Security) se inicie cuando se restaura el servidor de IBM Spectrum Protect. Si tiene una copia de seguridad, puede restaurar el archivo y reiniciar el servidor.

Procedimiento

Para crear una copia de seguridad de la base de datos de claves de certificados, `cert.kdb`, siga estos pasos:

1. Emita el mandato del servidor **DELETE KEYRING** para suprimir la información de la contraseña en la base de datos de claves de IBM Spectrum Protect.
2. Suprima todos los archivos `cert.*` restantes.
3. Cierre el servidor.
4. Inicie el servidor. El servidor crea automáticamente un nuevo archivo `cert.kdb` y una entrada correspondiente en la base de datos de IBM Spectrum Protect. Si no se emite el mandato **DELETE KEYRING**, el servidor intenta, en el arranque, crear la base de datos de claves con la contraseña anterior.

5. Redistribuya el nuevo archivo `.arm` en todos los clientes de copia de seguridad/archivado que utilicen TLS. Si está utilizando TLS 1.2, utilice el archivo `cert256.arm`. Utilice el archivo `cert.arm`, si el protocolo TLS que utiliza es anterior a 1.2. Reinstale todos los certificados de terceros en el cliente de copia de seguridad/archivado. Si está utilizando un servidor de directorio LDAP para autenticar las contraseñas, agregue el certificado raíz que se utilizó para firmar el certificado del servidor LDAP. Si el certificado raíz es ya un certificado de confianza predeterminado, no es necesario volver a agregarlo.

Qué hacer a continuación

Si no existe el archivo de base de datos de claves `cert.kdb`, el servidor lo creará. El archivo de opciones del servidor debe contar con la opción `SSLTCPPORT`, `SSLTCPADMINPORT` o ambas cuando se inicia el servidor. El servidor genera una contraseña modificable y un certificado autofirmado que puede extraerse para los clientes y los servidores de IBM business partners que van a utilizarse. Si el archivo `cert.kdb` ya existe y el servidor no lo crea, se produce una condición fuera de sincronización, que evita que el servidor establezca comunicaciones SSL.

Capítulo 6. Resolución de problemas del agente de almacenamiento

puede realizar una copia de seguridad y restaurar los datos de cliente directamente a y desde el almacenamiento adjunto a SAN utilizando el agente de almacenamiento.

Comprobación del registro de actividad del servidor para obtener información sobre el agente de almacenamiento

Compruebe el archivo de anotaciones de actividad del servidor y busque los informes correspondientes a los 30 minutos previos y a los 30 minutos posteriores al momento de producirse el error.

Los agentes de almacenamiento inician y gestionan muchas sesiones para el servidor. Revise el archivo de anotaciones de actividades del servidor para determinar si existen mensajes del agente de almacenamiento. Para revisar los mensajes de anotaciones de actividad, emita el mandato **QUERY ACTLOG**.

Si no aparece ningún mensaje en el archivo de anotaciones de actividades del servidor para este agente de almacenamiento, verifique los valores de comunicación:

- Emita el mandato `QUERY SERVER F=D` en el servidor y compruebe que la dirección de alto nivel (HLA) y la dirección de bajo nivel (LLA) establecidas para la entrada del servidor que representan a este agente de almacenamiento sean correctas.
- En el archivo de configuración de dispositivos especificado en el archivo `dsmsta.opt`, compruebe que SERVERNAME, así como HLA y LLA estén correctamente configurados en la línea **DEFINE SERVER**.

Compruebe si hay mensajes de error en el servidor para este agente de almacenamiento.

Resolución de un error provocado por la lectura o grabación en un dispositivo

Si el problema es un error que implica la lectura o grabación de datos de un dispositivo, muchos sistemas y dispositivos registran información en un archivo de anotaciones de errores del sistema.

El archivo de anotaciones de errores del sistema para AIX es errpt, y para Windows es el Registro de eventos.

Si un dispositivo o volumen utilizado por IBM Spectrum Protect informa de un error al archivo de registro de errores del sistema, se trata probablemente de un problema de dispositivos. Los mensajes de error registrados en el archivo de registro de errores del sistema pueden proporcionar información suficiente para resolver el problema.

Los agentes de almacenamiento son particularmente vulnerables si la información de la vía de acceso se ha cambiado y no es correcta. Emita el mandato **QUERY PATH**

F=D en el servidor. Verifique si los valores de cada una de las vías de acceso del agente de almacenamiento son correctas. En particular, verifique si el dispositivo indicado coincide con el nombre de dispositivo del sistema. Si la información de la vía de acceso no es correcta, actualice su información emitiendo el mandato **UPDATE PATH**.

Resolución de problemas causados por el cambio de opciones en el agente de almacenamiento

La realización de cambios en las opciones del archivo de opciones del agente de almacenamiento podría dar lugar a que las operaciones no se ejecuten correctamente aunque anteriormente hayan podido ejecutarse de forma correcta.

Revise cualquier cambio que se haya realizado en el archivo de opciones del agente de almacenamiento. Intente solucionar el problema volviendo a establecer los valores originales y volviendo a intentar la operación. Si el agente de almacenamiento ahora funciona correctamente, intente volver a especificar los cambios en el archivo de opciones del agente de almacenamiento de uno en uno y vuelva a intentar las operaciones del agente de almacenamiento hasta identificar el cambio realizado en el archivo de opciones que ha dado lugar al error.

Resolución de problemas causados por el cambio de la configuración o las opciones del servidor

Los cambios en el archivo de opciones del servidor o los cambios en la configuración del servidor que utilizan los mandatos **SET** puede afectar al agente de almacenamiento.

Revise cualquier cambio que se haya realizado en los valores de las opciones del servidor. Intente solucionar el problema volviendo a establecer los valores originales y volviendo a intentar la operación. Si el agente de almacenamiento ahora funciona correctamente, intente volver a especificar los cambios en el archivo de opciones del agente de almacenamiento de uno en uno y vuelva a intentar las operaciones del agente de almacenamiento hasta identificar el cambio realizado en el archivo de opciones que ha dado lugar al error.

Emita el mandato **QUERY STATUS** para revisar la configuración del servidor. Si se ha cambiado alguno de los valores de los que informa esta consulta, revise la razón del cambio y, si es posible, vuelva a establecerlos en los valores originales y vuelva a intentar la operación del agente de almacenamiento.

Configuración fuera de la LAN del agente de almacenamiento

El movimiento de datos sin LAN es el traspaso directo de datos del cliente entre un sistema cliente y un dispositivo de almacenamiento en una SAN, en lugar de una LAN. Es posible que tenga problemas con el agente de almacenamiento que están relacionados con la configuración fuera de la LAN.

Resolución de problemas relativos al envío de datos directamente al servidor

Las estadísticas de resumen del cliente no informan de ningún byte transferido fuera de la LAN.

Antes de empezar

El cliente informa de los bytes enviados fuera de LAN mediante la emisión del mandato "**ANE4971I LAN-free Data Bytes: xx KB**". De igual modo, el servidor no informa de ninguna instancia de "ANR0415I Session SESS_NUM proxied by *AGENTE_ALMACENAMIENTO* iniciada para el nodo *NOMBRE_NODO*" para este nodo y agente de almacenamiento, lo que indica que la operación de proxy fuera de la LAN se ha realizado para este nodo de cliente .

El cliente sólo intentará enviar datos fuera de la LAN con el agente de almacenamiento si el destino de la agrupación de almacenamiento primaria de la jerarquía de almacenamiento del servidor es un destino fuera de la LAN. Una agrupación de almacenamiento del servidor estará activada para el funcionamiento fuera de la LAN para un agente de almacenamiento determinado si se han definido una o varias vías de acceso desde ese agente de almacenamiento hasta un dispositivo de SAN.

Acerca de esta tarea

Para determinar si el destino de la agrupación de almacenamiento se ha configurado correctamente, realice los procedimientos siguientes:

Procedimiento

1. Emita el mandato **QUERY NODE** *nodeName* para informar del dominio de políticas al que se ha asignado este nodo.
2. Emita el mandato **QUERY COPYGROUP** *nombre_dominio nombre_juego_políticas nombre_clase_gestión* **F=D** para las clases de gestión que este nodo utilizaría desde su dominio de políticas asignado. Tenga en cuenta que este mandato transmite información relativa a los archivos de copia de seguridad. Para consultar información de grupos de copias de los archivos de copias archivadas, emita el mandato **QUERY COPYGROUP** *nombre_dominio nombre_juego_políticas nombre_clase_gestión* **TYPE=ARCHIVE F=D**.
3. Emita el mandato **QUERY STGPOOL** *nombre_grupo_almacenamiento*, donde *nombre_grupo_almacenamiento* es el destino del que se ha informado en consultas anteriores de **QUERY COPYGROUP**.
4. Emita el mandato **QUERY DEVCLASS** *nombre_clase_dispositivo* para la clase de dispositivo utilizada por el grupo de almacenamiento de destino.
5. Emita el mandato **QUERY LIBRARY** *nombre_biblioteca* para la biblioteca de la que se ha informado para la clase de dispositivo utilizada por el grupo de almacenamiento de destino.
6. Emita el mandato **QUERY DRIVE** *nombre_biblioteca* **F=D** para la biblioteca especificada para la clase de dispositivo utilizada por el grupo de almacenamiento de destino. Si no se han definido unidades para esta biblioteca, revise la configuración de la unidad y la biblioteca de este servidor y emita el mandato **DEFINE DRIVE** para definir las unidades necesarias. Si una o más de las unidades indican "ONLINE=No", evalúe por qué la unidad está desactivada y, si fuera posible, actívela mediante el mandato **UPDATE DRIVE** *libraryName driveName* **ONLINE=YES**.

7. Emita el mandato **QUERY SERVER** para determinar el nombre del agente de almacenamiento definido para este servidor.
8. Emita el mandato **QUERY PATH** *nombre_agente_almacenamiento*, donde *nombre_agente_almacenamiento* es el nombre del agente de almacenamiento definido para este servidor y del que se informa en el mandato **QUERY SERVER**. Revise esta salida y verifique si se han definido una o varias vías de acceso para las unidades definidas para la clase de dispositivo que la agrupación de almacenamiento de destino utiliza. Si no hay vías de acceso definidas para este grupo de almacenamiento, emita el mandato **DEFINE PATH** para definir las vías de acceso necesarias. Asimismo, revise esta salida y verifique si la vía de acceso está activada. Si se han definido vías de acceso pero no están activadas, active la vía de acceso mediante la emisión del mandato **UPDATE PATH** *nombre_origen nombre_destino* **SRCTYPE=SERVER DESTTYPE=DRIVE ONLINE=YES**.

Resolución de una agrupación de almacenamiento fuera de LAN inhabilitada

El servidor inhabilita una agrupación de almacenamiento como agrupación de almacenamiento activada fuera de la LAN si ésta se ha configurado para operaciones de grabación simultáneas.

En este caso, los datos del cliente se envían directamente a un servidor que no utilizará una agrupación de almacenamiento fuera de la LAN.

Emita el mandato **QUERY STGPOOL** *nombre_grupo_almacenamiento* **F=D** para el grupo de almacenamiento de destino de este cliente. Si la agrupación de almacenamiento se establece para las operaciones de grabación simultáneas, el valor "Agrupaciones de almacenamiento de copia:" hace referencia a uno o varios nombres de agrupaciones de almacenamiento distintos y IBM Spectrum Protect interpreta la operación de grabación simultánea para que tenga una prioridad mayor que la transferencia de datos fuera de la LAN. Puesto que se considera que la grabación simultánea es una operación que tiene una prioridad más alta, esta agrupación de almacenamiento no se notifica como agrupación de almacenamiento activada fuera de la LAN y, como tal, el cliente envía los datos directamente al servidor. El agente de almacenamiento no admite las operaciones de grabación simultánea.

Comprobación de la transferencia de datos a través de un entorno fuera de la LAN

El agente de almacenamiento y el cliente son capaces de gestionar la recuperación de error directamente en el servidor, en función de la configuración fuera de la LAN y del tipo de error detectado.

Dada esta capacidad de recuperación tras error, puede que no resulte aparente que los datos se están transfiriendo a través de la LAN cuando lo que se deseaba es que transfirieran fuera de ella. Es posible establecer el entorno fuera de la LAN para que la transferencia de datos quede limitada únicamente a la transferencia de datos fuera de la LAN.

Para probar una configuración fuera de la LAN, emita el mandato **UPDATE NODE** *nombre_nodo* **DATAWRITEPATH=LAN-FREE** para el nodo de cliente cuya configuración fuera de la LAN desee probar. A continuación, intente realizar una operación de almacenamiento de datos, como una copia de seguridad o una restauración. Si el cliente y el agente de almacenamiento intentan enviar los datos directamente al servidor mediante la utilización de la LAN, se recibirá el mensaje de error siguiente:

ANR0416W Session *sessionNumber* for node *nodeName* not allowed to *operation* using *path* data transfer path

La *operación* de la que se informa indica READ o WRITE, en función de la operación que ha intentado ejecutarse. La vía de acceso se notifica como vía de acceso fuera de la LAN.

Si se recibe este mensaje al intentar realizar una operación fuera de la LAN, evalúe y verifique los valores del funcionamiento fuera de la LAN. Por lo general, si los datos no se envían fuera de la LAN, el cliente se ha configurado para utilizar el funcionamiento fuera de la LAN, el destino de la agrupación de almacenamiento para la política asignada a este nodo no es una agrupación de almacenamiento activada para el funcionamiento fuera de la LAN o las vías de acceso no se han definido correctamente.

Capítulo 7. Utilización del rastreo para resolver problemas

IBM Spectrum Protect puede, en ocasiones, experimentar problemas que podrá resolver mediante el rastreo.

Inicio de un rastreo ampliado del Centro de operaciones

AIX Linux Windows

De forma predeterminada, el registro del centro de operaciones contiene datos de un rastreo básico de los sucesos del centro de operaciones. Es posible que el servicio de soporte de software de IBM le solicite que inicie un rastreo ampliado.

Acerca de esta tarea

Para iniciar un rastreo ampliado del centro de operaciones, siga uno de los procedimientos siguientes:

Conceptos relacionados:

"Visión general de los archivos de registro" en la página 107

Tareas relacionadas:

"Visualización del registro del Centro de operaciones en el Centro de operaciones" en la página 108

Rastreo del Centro de operaciones habilitando las funciones de registro desde el Centro de operaciones

AIX Linux Windows

En el centro de operaciones puede habilitar las funciones de registro e iniciar un rastreo ampliado que añada datos de resolución de problemas al registro del centro de operaciones.

Acerca de esta tarea

En el procedimiento siguiente, habilitará grupos de funciones de registro e iniciará un rastreo ampliado.

Atención: Asegúrese de que inhabilita los grupos después del rastreo. De lo contrario, el rendimiento del centro de operaciones puede verse afectado.

Procedimiento

Para rastrear el centro de operaciones, siga estos pasos:

1. En la barra de menús del centro de operaciones, pase el puntero sobre el icono de signo de interrogación y seleccione **Acerca del Centro de operaciones**.
2. Pulse **Detalles de instalación**.
3. Pulse el separador **Registro**.
4. En la lista de grupos de registro, seleccione las filas que le solicite el servicio de soporte de software de IBM y pulse **Habilitar**.
5. Confirme que desea habilitar los grupos de registro y pulse **Cerrar**.

6. Vuelva a crear el problema que está intentando resolver. Automáticamente se rastreará el centro de operaciones y se creará una nueva versión del registro del centro de operaciones.
7. Vuelva a la lista de grupos de registro repitiendo el paso 1 en la página 123 - paso 3 en la página 123.
8. Seleccione todas las filas habilitadas y pulse **Inhabilitar**.
9. Confirme que desea inhabilitar los grupos de registro y pulse **Cerrar**.

Qué hacer a continuación

Para obtener la ubicación y los nombres de los archivos de registro del centro de operaciones, consulte "Visión general de los archivos de registro" en la página 107.

Tareas relacionadas:

"Visualización del registro del Centro de operaciones en el Centro de operaciones" en la página 108

"Rastreo del Centro de operaciones habilitando las funciones en el archivo de configuración del registro"

Rastreo del Centro de operaciones habilitando las funciones en el archivo de configuración del registro

AIX Linux Windows

Si el problema que está resolviendo le impide abrir el centro de operaciones, puede abrir y modificar el archivo de configuración del registro e iniciar un rastreo ampliado que añada los datos al registro del centro de operaciones.

Acerca de esta tarea

En el procedimiento siguiente, habilitará grupos de funciones de registro e iniciará un rastreo ampliado.

Atención: Asegúrese de que inhabilita los grupos después del rastreo. De lo contrario, el rendimiento del centro de operaciones puede verse afectado.

Procedimiento

Para rastrear el centro de operaciones, siga estos pasos:

1. Detenga el servidor web del centro de operaciones.
2. Vaya al directorio siguiente:

   AIX Linux *installation_dir*/ui/Liberty/usr/servers/guiServer

   Windows *installation_dir*\ui\Liberty\usr\servers\guiServer

   donde *installation_dir* es el directorio en el que se ha instalado IBM Spectrum Protect.
3. Guarde una copia del archivo de configuración de registro, `OpsCntrLog.config`, en otra ubicación para utilizarla posteriormente.
4. Abra el archivo `OpsCntrLog.config` original en un editor de texto.
5. En el editor de texto, habilite únicamente los grupos de registro que le solicite el servicio de soporte de software de IBM sustituyendo la palabra `OFF` por la palabra `ON` en cada grupo relevante.
6. Guarde y cierre el archivo.

7. Inicie el servidor web del centro de operaciones.
8. Vuelva a crear el problema que está intentando resolver. Automáticamente se rastreará el centro de operaciones y se creará una nueva versión del registro del centro de operaciones.
9. Detenga el servidor web del centro de operaciones.
10. Vuelva al directorio `guiServer`.
11. Inhabilite los grupos de registro sustituyendo el archivo `OpsCntrLog.config` editado por la copia que ha guardado anteriormente.
12. Inicie el servidor web del centro de operaciones.

Qué hacer a continuación

Para obtener la ubicación y los nombres de los archivos de registro del centro de operaciones, consulte "Visión general de los archivos de registro" en la página 107.

Tareas relacionadas:

"Rastreo del Centro de operaciones habilitando las funciones de registro desde el Centro de operaciones" en la página 123

Habilitación del rastreo para el servidor o el agente de almacenamiento

Puede emitir mandatos de rastreo desde los siguientes lugares: la consola del servidor, la consola del agente de almacenamiento, el cliente de administración conectado al servidor o al agente de almacenamiento, el archivo de opciones del servidor (`dsmserv.opt`) o el archivo de opciones del agente de almacenamiento (`dsmsta.opt`).

Antes de empezar

Los mandatos de rastreo se aplican al servidor o al agente de almacenamiento al que se envía el mandato. Los mandatos de rastreo en los archivos de opciones se utilizan para rastrear las aplicaciones durante el inicio o inicialización de las aplicaciones o para proporcionar un conjunto predeterminado de clases de rastreo. Existe una clase de rastreo (**ADDMSG**) que está siempre habilitada de forma predeterminada, independientemente de si aparece en el archivo de opciones o no. Es preferible realizar el rastreo en un archivo. Por lo general, el rastreo para el servidor o el agente de almacenamiento generará una salida de gran tamaño.

Acerca de esta tarea

Realice los pasos siguientes para activar clases de rastreo para el servidor o el agente de almacenamiento:

Procedimiento

1. Determine las clases de rastreo que desea activar. Para poder emitir mensajes de rastreo para una clase de rastreo determinada, es necesario que esa clase de rastreo esté activada o bien antes del comienzo del rastreo o bien después de que se haya iniciado el rastreo.
2. Emita el mandato **TRACE ENABLE** *nombre_clase_rastreo* para habilitar una o varias clases de rastreo. Tenga en cuenta que *nombre_clase_rastreo* puede ser una lista clases de rastreo delimitada por espacios. Por ejemplo, este mandato se podría especificar como **TRACE ENABLE TM SESSION**. El mandato **TRACE ENABLE** es acumulativo, de manera que las clases de rastreo extra se pueden activar

mediante la emisión de **TRACE ENABLE** varias veces. Por ejemplo, si deseaba agregar la clase de rastreo PVR además de las que ya están habilitadas, emita: **TRACE ENABLE PVR**. Para dejar de emitir mensajes de rastreo para una clase de rastreo determinada, es necesario que esa clase de rastreo esté desactivada o bien antes del comienzo del rastreo o bien después de que se haya iniciado el rastreo.

3. Emita el mandato **TRACE DISABLE**<*nombre_clase_rastreo*> para inhabilitar una o más clases de rastreo. Tenga en cuenta que *nombre_clase_rastreo* puede ser una lista delimitada por espacios de clases de rastreo. Por ejemplo, este mandato se podría especificar como **TRACE DISABLE TM SESSION**. Las clases de rastreo adicionales también se pueden desactivar mediante la emisión de **TRACE DISABLE**. Por ejemplo, si deseaba suprimir la clase de rastreo PVR además de las que ya estaban desactivadas, emita: **TRACE DISABLE PVR**. Al emitir **TRACE DISABLE** sin especificar clases de rastreo, todas las clases de rastreo activadas actualmente se desactivan.
4. El rastreo puede realizarse en la consola o en un archivo. Lleve a cabo las siguientes tareas para comenzar el rastreo:
   - Para rastrear a la consola, emita: **TRACE BEGIN**
   - Para rastrear a un archivo sin limitación de tamaño, emita: **TRACE BEGIN** *nombre_archivo*
   - Para rastrear a un archivo con limitación de tamaño, emita: **TRACE BEGIN** *nombre_archivo* **MAXSIZE=** *tamaño máximo en megabytes*

   Nota: El *nombre_archivo* puede ser una vía de acceso completamente calificada como `/opt/tmp` o `c:\temp`. Si no se especifica una vía de acceso completa, el archivo de rastreo se colocará en el mismo directorio que el archivo ejecutable activo.
5. Realice la operación que está causando el problema.
6. Emita el mandato **TRACE END** para detener la emisión de mensajes de rastreo. Si el rastreo se realiza en un archivo, la detención del rastreo graba los mensajes de rastreo restantes en el archivo y cierra el archivo.

Qué hacer a continuación

Es posible activar el rastreo e iniciarlo utilizando el archivo de opciones del servidor o del agente de almacenamiento. Los mandatos y la sintaxis descritos son idénticos para el archivo de opciones del servidor o del agente de almacenamiento y generalmente se utilizan para el rastreo durante el inicio e inicialización del servidor. Por ejemplo, si se han agregado las líneas siguientes al archivo de opciones del servidor, el rastreo comenzaría para las clases de rastreo DB, TM y LOG, y los mensajes de rastreo grabados en el archivo `MYTRACE.OUT`.

```
TRACE ENABLE DB TM LOG
TRACE BEGIN MYTRACE.OUT BUFSIZE=4096
```

Recuerde: Si está realizando un rastreo debido al bloqueo de un servidor, no establezca el parámetro **BUFSIZE**.

Referencia relacionada:

"Clases de rastreo de agente de almacenamiento y de servidor" en la página 128

Habilitar el rastreo de pila para los mensajes del servidor o el agente de almacenamiento

Un rastreo de pila proporciona información sobre una aplicación que puede ayudar al servicio de soporte de IBM a diagnosticar los problemas de una forma más rápida.

Nota: Dependiendo de la frecuencia del fracaso, el rastreo de la pila puede saturar el archivo de registro de la actividad, que puede provocar problemas al intentar ver el archivo de registro de la actividad. Es posible que desee desactivar el rastreo de la pila después de que finalice.

La asistencia de software de IBM podría resultarle útil para habilitar el rastreo de pila en mensajes específicos emitidos por el servidor o el agente de almacenamiento. Los tipos de mensajes en los que un rastreo de pila puede habilitarse son la consola del servidor, la consola del agente de almacenamiento y el cliente administrativo que está conectado al servidor o al agente de almacenanamiento.

Para obtener un rastreo de pila cuando el servidor o el agente de almacenamiento emite un mensaje específico, active el mensaje del rastreo de pila. Emita el mandato **MSGSTACKTRACE ENABLE** <*número_mensaje*> para habilitar uno o más mensajes para el rastreo de pila.

Recuerde: <*número_mensaje*> puede ser una lista de números de mensaje delimitada por espacios.

Este mandato puede escribirse como **MS ENABLE 2017**. El mandato **MSGSTACKTRACE ENABLE** es acumulativo, como los mensajes extra que se habilitan emitiendo el mandato **MSGSTACKTRACE ENABLE** más veces. Si quiere añadir el mensaje 985, a los mensajes que ya se han habilitado, emita **MS ENABLE 985**. Observe que únicamente se permite la parte de número del mensaje en el mandato **MSGSTACKTRACE**. Para detener el rastreo de la pila para los mensajes que emite el servidor o el agente de almacenamiento el rastreo de la pila para estos mensajes debe estar deshabilitado. Emita el mandato **MSGSTACKTRACE DISABLE** <*número_mensaje*> para inhabilitar uno o varios mensajes.

El <*messageNumber*> puede ser una lista de espacios delimitados de números de mensajes. Por ejemplo, este mandato puede introducirse como **MSGSTACKTRACE DISABLE 2017 985**. Los mensajes adicionales también se pueden desactivar emitiendo **MS DISABLE**. Por ejemplo, si desea eliminar el número de mensaje 7837 además de los mensajes que ya están deshabilitados, emita el mandato **MSGSTACKTRACE DISABLE 7837**.

Los siguientes mensajes están habilitados de forma predeterminada para el rastreo de pila.

```
435 437 486 661 685 727 728 780 781 782
784 785 786 790 793 794 860 881 882 883
884 1032 1078 1092 1117 1156 1227 5010 5015 5019
5021 5093 5099 5100 5267 6753 7823 7837 9600 9601
9602 9604 9605 9606 9607 9608 9999
```

Clases de rastreo de agente de almacenamiento y de servidor

El cliente y el agente de almacenamiento proporcionan clases de rastreo agregadas. Estas clases de rastreo son métodos abreviados para utilizar muchas clases de rastreo relacionadas indicando un nombre de clase de rastreo agregada para el mandato **TRACE ENABLE**.

Las clases de rastreo que aparecen en Tabla 10 son esas clases de rastreo que se solicitan o utilizan de forma más común para diagnosticar problemas. Esta lista no incluye todas las clases de rastreo posibles que están disponibles. El nombre de la clase de rastreo se utiliza con los mandatos **TRACE ENABLE** y **TRACE DISABLE**.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor

Clases de rastreo	Descripción	Uso
ADDMSG	Emite mensajes de la consola, tales como los mensajes ANR y ANE, para el archivo de rastreo.	Esta clase de rastreo es útil para correlacionar mensajes de servidor con mensajes de rastreo, y para conservar el momento en el cual se emitió cada uno.
ADMCMD	Rastreos relacionados con el proceso de mandatos.	Utilice esta clase de rastreo para depurar el intérprete de mandatos, incluido el manejo de los mandatos **PARALLEL** y **SERIAL**.
AF	Esta clase de rastreo muestra información sobre los datos de usuario que se guardan en dispositivos de medios secuenciales. AF es una clase de rastreo agregada que utiliza AFCREATE, AFMOVE, AFLOCK, AFTXN y AFCOPY. Emita **TRACE DISABLE AFLOCK** a menos que la información de bloqueo se requiera o necesite explícitamente.	Utilice esta clase de rastreo para diagnosticar problemas sobre cómo leer o grabar los archivos de usuario en volúmenes de medios secuenciales.
AFCREATE	Esta clase de rastreo muestra información sobre el almacenamiento de datos de usuario en volúmenes de medios secuenciales.	Utilice esta clase de rastreo para realizar el diagnóstico de grabación de archivos de usuario en volúmenes de medios secuenciales.
AFMOVE	Esta clase de rastreo muestra operaciones que traspasan datos de usuario con volúmenes de medios secuenciales. Las operaciones de traspaso se realizan mediante los procesos de servidor MIGRATION, RECLAMATION, MOVE DATA y MOVE NODEDATA.	Utilice esta clase de rastreo para realizar el diagnóstico de problemas de procesos de servidor de traspaso de datos.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
AS	Esta clase de rastreo muestra información sobre selección y asignación de volúmenes, coordinación de unidades (puntos de montaje) y gestión de ubicación de datos en volúmenes. Se trata de una clase de rastreo agregada que utiliza ASALLOC, ASRTRV, ASDEALLOC, ASMOUNT, ASVOL, ASTXN y ASSD. El método típico es emitir TRACE DISABLE ASTXN, a menos que la información de bloqueo se solicite o necesite de forma explícita.	Utilice esta clase de rastreo para diagnosticar muchos problemas distintos sobre volúmenes, puntos de montaje u operaciones de lectura y grabación de datos.
ASALLOC	Esta clase de rastreo muestra información sobre la reserva y la asignación de espacio en volúmenes de medios secuenciales para almacenar datos. Este espacio puede ser para almacenar datos en nombre de una sesión de cliente o para operaciones de traspaso de datos de servidor como MIGRATION, RECLAMATION, MOVE DATA o MOVE NODEDATA.	Diagnosticar problemas por los cuales el servidor o el agente de almacenamiento informan de que no hay espacio disponible, pero se supone que hay espacio disponible en la jerarquía de almacenamiento.
ASDEALLOC	Esta clase de rastreo muestra información sobre la liberación y la desasignación de espacio en volúmenes de medios secuenciales para almacenar datos. Algunas operaciones típicas de desasignación en el servidor son **EXPIRATION**, **MIGRATION**, **RECLAMATION**, **MOVE DATA**, **MOVE NODEDATA**, **AUDIT VOLUME**, **DELETE VOLUME** y **DELETE FILESPACE**.	Utilice esta clase de rastreo para realizar el diagnóstico durante la eliminación de datos.
ASMOUNT	Esta clase de rastreo muestra información sobre selección de unidad (punto de montaje) y asignación de dispositivos de medios secuenciales.	Las situaciones de diagnóstico en las cuales las sesiones o los procesos se encuentran en espera de punto de montaje o casos en los cuales una operación falla porque no hay ningún punto de montaje disponible. También resulta útil en casos en los que se adelanta un punto de montaje.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
ASRTRV	Esta clase de rastreo muestra información sobre la lectura de datos desde volúmenes de medios secuenciales.	Utilice esta clase de rastreo para diagnosticar problemas sobre datos como el cliente de **RESTORE** o **RETRIEVE** mediante el cliente o **MIGRATION**, **RECLAMATION**, **STORAGE POOL BACKUP**, **AUDIT VOLUME**, **GENERATE BACKUPSET**, **EXPORT**, **MOVE DATA**, or **MOVE NODEDATA** mediante el servidor.
ASTXN	Esta clase de rastreo muestra información sobre transacciones que se utilizan para hacer actualizaciones de la base de datos de información para los volúmenes de medios las agrupaciones de almacenamiento y otros atributos.	Utilice esta clase de rastreo para diagnosticar situaciones en las que una aplicación deja de responder, operaciones de base de datos, errores en operaciones de medios secuenciales o problemas de almacenamiento de datos en general.
ASVOL	Esta clase de rastreo muestra información sobre selección de volumen y asignación de volúmenes de medios secuenciales.	Utilice esta clase de rastreo para diagnosticar situaciones en las cuales las sesiones o los procesos se encuentran en espera de volúmenes o casos en los cuales una operación falla porque no hay ningún volumen disponible. También resulta útil en casos en los que se adelanta un acceso de volumen.
ASSD	Esta clase de rastreo muestra información sobre las operaciones de datos de corriente secuenciales. Estas operaciones utilizan clases de dispositivo, volúmenes o puntos de montaje de medios secuenciales, pero que no almacenan datos en la jerarquía de almacenamiento. Los procesos de servidor que completan operaciones de datos de corriente secuenciales son BACKUP DB, EXPORT/IMPORT y GENERATE BACKUPSET.	Utilice esta clase de rastreo para diagnosticar procesos de servidor que completan las operaciones de datos secuenciales.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
BF	Información sobre los datos de usuario (archivos) almacenados en la jerarquía de almacenamiento. Esta clase de rastreo agregada utiliza **BFCREATE**, **BFRTRV**, **BFSALVAGE**, **BFLOCK**, **BFAGGR**, **BFREMOTE**, **BFSAGGR**, y **BFTRG**.	Utilice esta clase de rastreo para diagnosticar problemas generales de lectura o grabación de datos en las operaciones de cliente y los procesos de servidor.
BFAGGR	Esta clase de rastreo muestra información sobre la agregación del servidor de datos de usuario. El servidor añade muchos archivos de usuario más pequeños en un archivo de mayor tamaño en la jerarquía de almacenamiento para optimizar el rendimiento de las operaciones de traspaso de datos como **MIGRATION**, **MOVE DATA** y **MOVE NODEDATA**.	Utilice esta clase de rastreo para diagnosticar problemas generales de lectura o grabación de datos en las operaciones de cliente y los procesos de servidor, o ambos a la vez.
BFCREATE	Esta clase de rastreo muestra información sobre operaciones de cliente que almacenan datos en la jerarquía de almacenamiento. Estas operaciones de cliente suelen ser **BACKUP**, **ARCHIVE** u operaciones **SPACE MANAGE** del cliente.	Utilice esta clase de rastreo para diagnosticar errores u otros problemas durante el almacenamiento de datos por parte del cliente.
BFREMOTE	Rastrea la primera fase de los procesos de restauración y copia de seguridad de NDMP (Network Data Management Protocol).	Esta clase de rastreo se utiliza para identificar operaciones de copia de seguridad o restauración relacionadas con NDMP. Estas clases de rastreo son específicas para las funciones que implementan el protocolo NDMP. La clase de rastreo SPID ofrece un rastreo más detallado, incluido el rastreo del historial del registro de archivos NDMP que se envía al servidor de archivos NDMP.
BFRTRV	Esta clase de rastreo muestra información sobre operaciones de cliente que lee datos desde la jerarquía de almacenamiento.	Utilice esta clase de rastreo para diagnosticar errores u otros problemas durante la lectura de datos por parte del cliente.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
BFSAGGR	Esta clase de rastreo muestra información sobre almacenamiento, recuperación y traslado de superagregados. Un objeto más grande de 10 GB se guarda como superagregado.	Utilice esta clase de rastreo para diagnosticar problemas relacionados con el almacenamiento y la recuperación de objetos superiores a 10 GB.
BITVECTOR	Diagnostica problemas en los casos en que el servidor notifica la existencia de problemas en las agrupaciones de almacenamiento en disco.	Utilice esta clase de rastreo para mostrar información acerca de la reserva y la asignación de espacio en volúmenes de agrupaciones de almacenamiento en disco.
BKSET/OBJSET	Clases de rastreo para funciones de conjunto de copias de seguridad. Las clases de rastreo BKSET y OBJSET son sinónimas.	Utilice esta clase de rastreo para depurar problemas con el mandato GENERATE BACKUPSET o durante una operación de restauración de cliente desde un juego de copias de seguridad.
BLKDISK	Clase de rastreo para visualizar la actividad E/S de disco de agrupación de almacenamiento, base de datos y volúmenes de anotaciones.	Utilice esta clase de rastreo para visualizar la actividad E/S de disco para diagnosticar el rendimiento y errores de E/S de disco.
BRNODE	La clase de rastreo para los mandatos **BACKUP** y **RESTORE NODE**, que se utilizan durante las operaciones NDMP.	Utilice esta clase de rastreo para depurar problemas con los mandatos **BACKUP** y **RESTORE NODE**.
COLLOCATE	Esta clase de rastreo muestra información sobre el proceso de proximidad en agrupaciones de almacenamiento. La clase de rastreo COLLOCATEDETAIL también se puede utilizar para conseguir información más detallada sobre el proceso de colocación. Por ejemplo, la información sobre los archivos que se procesan para un grupo de colocación. Los archivos que se están procesando para un grupo de colocación pueden producir muchas sentencias de rastreo de salida.	Utilice esta clase de rastreo para realizar el diagnóstico de problemas del proceso de proximidad.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
CRC	Esta clase de rastreo muestra información sobre la generación y la gestión de comprobaciones de redundancia cíclicas (CRC) en el servidor o en el agente de almacenamiento. CRC es una clase de rastreo de agregaciones que utiliza **CRCDATA**, **CRCPROTO** y **CRCVAL**.	Utilice esta clase de rastreo para diagnosticar problemas de datos dañados, cuando el proceso de CRC no ha informado de la presencia de datos dañados.
CRCDATA	Esta clase de rastreo muestra información sobre cómo generar y gestionar CRC para los datos que se almacenan en las agrupaciones de almacenamiento con el conjunto `CRCDATA=YES`.	Utilice esta clase de rastreo para diagnosticar problemas de datos dañados, cuando el proceso de CRC no ha informado de la presencia de datos dañados.
CRCPROTO	Esta clase de rastreo muestra información sobre cómo generar y gestionar CRC para los datos intercambiados entre el cliente y el servidor o el agente de almacenamiento donde este nodo está configurado con `VALIDATEPROTOCOL=ALL` o `VALIDATEPROTOCOL=DATAOnly` en el servidor.	Utilice esta clase de rastreo para diagnosticar problemas de datos dañados, cuando el proceso de CRC no ha informado de la presencia de datos dañados.
CRCVAL	Esta clase de rastreo muestra información sobre la generación y la comparación de valores CRC.	Informativo para mostrar valores CRC durante el proceso.
CRYPTO	Esta clase de rastreo muestra información sobre las operaciones de AES (advanced encryption standard) y algunos valores de cifrado general.	Utilice esta clase de rastreo para aislar e identificar los problemas relacionados con el cifrado.
DBCLI	Rastrea el conjunto general de interacciones.	Utilice esta clase de rastreo para rastrear el conjunto general de interacciones de DB2 y la compatibilidad de la interfaz de línea de mandatos de DB2.
DBCONN	Rastrea las actividades de conexión.	Utilice esta clase de rastreo para rastrear las conexiones de IBM Spectrum Protect con las conexiones de DB2. Esta clase de rastreo muestra, por ejemplo, la creación de los descriptor de conexión y la asignación de conexiones a las transacciones.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
DBDBG	Procesos de depuración de rastreo. Puede utilizar esta clase de rastreo primero cuando depure un problema en una base de datos.	Utilice esta clase de rastreo para mostrar la entrada o salida de funciones, los códigos de retorno de salida y las sentencias que se han creado y se están ejecutando.
DBITXN	Rastrea las actividades relacionadas con las transacciones en la base de datos. Las actividades relacionadas con transacciones comprenden la adquisición y la liberación de mecanismos de cierre de transacciones, la asignación y la liberación de dbTxnDesc y el proceso de confirmaciones de transacciones a partir de las funciones de las fases de confirmación y preparación.	Utilice esta clase de rastreo para rastrear las actividades relacionadas con transacciones de la interfaz de la base de datos.
DBNETDB	Esta clase de rastreo muestra información sobre operaciones fuera de la LAN, y la negociación y gestión de información entre el servidor y el agente de almacenamiento.	Utilice esta clase de rastreo para diagnosticar problemas sin LAN cuando el servidor y el agente de almacenamiento estén en niveles diferentes. Funcionan mejor cuando están en el mismo nivel. También puede utilizar esta clase de rastreo para diagnosticar problemas con el agente de almacenamiento que obtiene la información de configuración desde el servidor.
DBRC	Rastrea los códigos de retorno de funciones del componente de la base de datos.	Utilice esta clase de rastreo para rastrear los códigos de retorno.
DEDUP	Rastrea la vía de acceso lógica general del proceso de desduplicación de datos. Normalmente no incluye vías de acceso de errores.	Utilice DEDUP para rastrear vías de acceso lógicas para el proceso de desduplicación de datos.
DEDUP1	Rastrea las vías de acceso de errores para el proceso de desduplicación de datos.	Utilice DEDUP1 para rastrear vías de acceso de errores para el proceso de desduplicación de datos.
DEDUP2	Rastrea la vía de acceso de huellas dactilares y firmas digitales.	Utilice DEDUP2 para rastrear vías de acceso de huellas dactilares y firmas digitales.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
DELTA	Clase de rastreo para funciones de grupo lógico. Las clases de rastreo DELTA y GROUP son sinónimas.	Utilice esta clase de rastreo para depurar problemas con grupos lógicos, ya sean grupos diferenciales básicos (copia de seguridad de subarchivos) o grupos de homólogos (Windows SYSTEM OBJECT o copias de seguridad de imagen). El proceso de grupos es relevante durante cualquier operación que haga referencia a objetos de copia de seguridad. Los objetos de copia de seguridad pueden incluir la copia de seguridad del cliente y la restauración, la caducidad, la supresión (**DELETE FILESPACE**, **DELETE VOLUME**), la exportación/importación, la generación y restauración de juegos de copias de seguridad, la restauración sin consulta, la auditoría de bases de datos, etc.
DF	Esta clase de rastreo muestra información sobre los datos de usuario que se guardan en los volúmenes de disco. DF es una clase de rastreo de agregación que activa **DFCREATE**, **DFRTRV**, **DFMOVE**, **DFLOCK**, **DFTXN** y **DFCOPY**. Emita el mandato **TRACE DISABLE DFLOCK** a menos que la información de bloqueo se requiera o necesite explícitamente.	Utilice esta clase de rastreo para diagnosticar problemas sobre lectura o grabación de los archivos de usuario a los volúmenes de disco.
DFCREATE	Esta clase de rastreo muestra información sobre el almacenamiento de datos de usuario en volúmenes de disco.	Utilice esta clase de rastreo para realizar el diagnóstico de grabación de archivos de usuario en volúmenes de disco.
DFMOVE	Esta clase de rastreo muestra operaciones que traspasan datos de usuario utilizando volúmenes de disco. Las operaciones de traspaso se completan mediante los procesos de servidor MIGRATION, MOVE DATA y MOVE NODEDATA.	Utilice esta clase de rastreo para realizar el diagnóstico de problemas de procesos de servidor de traspaso de datos.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
DFRTRV	Esta clase de rastreo muestra información sobre la lectura de datos de usuario desde volúmenes de disco.	Utilice esta clase de rastreo para realizar el diagnóstico de lectura de archivos de usuario en volúmenes de disco.
DS	Esta clase de rastreo muestra información sobre selección de volumen, reserva de espacio, asignación, y gestión de ubicación de datos en volúmenes de disco. DS es una clase de rastreo agregada que activa DSALLOC, DSRTRV, DSDEALLOC y DSVOL. Emita **TRACE DISABLE DSTXN** a menos que la información de bloqueo se requiera o necesite explícitamente.	Utilice esta clase de rastreo para diagnosticar muchos problemas diferentes sobre las operaciones de lectura y grabación de los datos de volumen de disco.
DSALLOC	Esta clase de rastreo muestra información sobre la reserva y la asignación de espacio en volúmenes de disco para almacenar datos. Es posible que el almacenamiento de disco se complete en nombre de una sesión de cliente o para las operaciones de traslado de datos como **MIGRATION**, **MOVE DATA** o **MOVE NODEDATA**.	Diagnosticar problemas donde el servidor o el informe de agente de almacenamiento informan de que no hay espacio disponible, pero parece que hay espacio disponible en la jerarquía de almacenamiento.
DSDEALLOC	Esta clase de rastreo muestra información sobre la liberación y la desasignación de espacio en volúmenes de disco. Algunas operaciones típicas de desasignación en el servidor son **EXPIRATION**, **MIGRATION**, **MOVE DATA**, **MOVE NODEDATA**, **AUDIT VOLUME**, **DELETE VOLUME** y **DELETE FILESPACE**.	Utilice esta clase de rastreo para realizar el diagnóstico durante la eliminación de datos.
DSRTRV	Esta clase de rastreo muestra información sobre la lectura de datos desde volúmenes de disco.	Utilice esta clase de rastreo para diagnosticar problemas relacionados con la lectura de datos como **RESTORE** o **RETRIEVE** mediante el cliente o bien **MIGRATION**, **STORAGE POOL BACKUP**, **AUDIT VOLUME**, **GENERATE BACKUPSET**, **EXPORT**, **MOVE DATA**, o **MOVE NODEDATA** mediante el servidor.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
DSVOL	Esta clase de rastreo muestra información sobre selección de volumen y asignación para volúmenes de disco.	Utilice esta clase de rastreo para diagnosticar situaciones en las cuales las sesiones o los procesos se encuentran en espera de volúmenes o casos en los cuales una operación falla porque no hay ningún volumen disponible.
ICVOLHST	Clase de rastreo para funciones de histórico de volúmenes.	Utilice esta clase de rastreo para depurar problemas cuando crea entradas históricas de volúmenes, por ejemplo, mediante **EXPORT**, **BACKUP DB** o **GENERATE BACKUPSET**, o al suprimir entradas históricas de volúmenes, por ejemplo mediante **DELETE VOLHISTORY**.
IMFS	Clases de rastreo para funciones de espacio de archivos.	Utilice esta clase de rastreo para depurar problemas relacionados con espacios de inventario (por ejemplo, durante **DELETE FILESPACE**).
LANFREE	Esta clase de rastreo muestra información general sobre operaciones fuera de la LAN en el servidor o el agente de almacenamiento. Igualmente, muestra información de error para operaciones relacionadas fuera de la LAN. LANFREE es una clase de rastreo agregada que activa LNFVERB, LNFMEM, LNFENTRY y LNFDATA.	Cualquier error de fuera de la LAN.
MMS	Esta clase de rastreo muestra información sobre las bibliotecas de cintas y el servidor o sobre el agente de almacenamiento que utiliza estas bibliotecas.MMS es una clase de rastreo agregada que activa MMSBASE, MMSTXN, MMSLIB, MMSDRIVE, MMSOP, MMSMAN, MMSSCSI, MMSFLAG, MMSACSLS y MMSSHARE. Incluye las clases de rastreo NA y PVR al rastrear MMS.	Se utiliza para diagnosticar problemas con las bibliotecas de cintas, inventarios de volúmenes de biblioteca u otros problemas de bibliotecas en general.
MONITOR	Esta clase de rastreo muestra información sobre la supervisión de alertas.	Utilice esta clase de rastreo para determinar por qué es posible que una alerta no se genere.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
NA	Esta clase de rastreo muestra información sobre información de ruta para el servidor o el agente de almacenamiento. Esta información está relacionada con los mandatos **DEFINE PATH**, **UPDATE PATH**, **DELETE PATH** y **QUERY PATH**. Esta clase de rastreo también se utiliza para identificar problemas que están relacionados con operaciones que incluyen servidores de archivos NDMP, por ejemplo, **DEFINE DATAMOVER**, **UPDATE DATAMOVER**, **BACKUP NODE** y **RESTORE NODE**. Esta clase de rastreo agregada utiliza NALOCK, NAPATH, NAMOVER, NADISK y NACONFIG. Quizá sea mejor incluir las clases de rastreo MMS y PVR cuando rastrea NA.	Utilice esta clase de rastreo para realizar el diagnóstico de problemas de vías de acceso a dispositivos.
PRODCONS	Si hay problemas con el funcionamiento de los lotes asignados, PRODCONS muestra información sobre el problema y sobre si está en el objeto del PC o en réplica.	Utilice PRODCONS para rastrear el funcionamiento interno de los objetos de producción/consumo que se utilizan en el servidor.
PROXYNODE	Esta clase de rastreo muestra información sobre las sesiones proxynode y los mandatos relacionados a las asociaciones proxynode (GRANT, REVOKE, QUERY PROXYNODE).	Utilice esta clase de rastreo para realizar el diagnóstico de problemas de sesiones proxynode y mandatos relacionados. Quizá sea mejor incluir el rastreo SESSION al analizar los problemas de sesión de proxynode.
PVR	Esta clase de rastreo muestra información sobre dispositivos de medios secuenciales y el uso de ellos por parte del servidor y del agente de almacenamiento. PVR es una clase de rastreo agregada que activa PVRVOL, PVRCLASS y PVRMP. La clase de rastreo PVR contiene todo lo contenido en la clase de rastreo agregada PVRIO y en la clase de rastreo PVRNOIO.	Utilice esta clase de rastreo para diagnosticar problemas con unidades de cintas, fallos de lectura o grabación de volúmenes de cintas u otros problemas relacionados con los volúmenes de cintas.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
PVRIO	Esta clase de rastreo muestra rastreo de operaciones de lectura, grabación o POS para dispositivos de medios secuenciales y el uso de ellos por parte del servidor y del agente de almacenamiento.	Utilice esta clase de rastreo para diagnosticar problemas con fallos de unidades de cintas al leer o grabar volúmenes de cintas.
PVRNOIO	Esta clase de rastreo muestra información PVRVOL, PVRCLASS y PVRMP.	Utilice esta clase de rastreo para diagnosticar problemas con montajes de unidades de cintas u otros problemas relacionados con los volúmenes de cintas.
REPL	REPL es una clase de rastreo agregada que activa REPLBATCH, REPLCMD, REPLFS, REPLINV, REPLPROC, REPLSTATS y REPLSESS.	Utilice esta clase de rastreo para realizar el diagnóstico de problemas con replicación.
REPLBATCH	Esta clase de rastreo muestra el rastreo relacionado con el proceso por lotes, donde los archivos individuales se envían desde el servidor de origen al servidor de destino.	Utilice esta clase de rastreo para diagnosticar problemas de replicación con el proceso por lotes.
REPLCMD	Esta clase de rastreo muestra el rastreo relacionado con el análisis de mandatos y la resolución de reglas de replicación de espacio de archivos.	Utilice esta clase de rastreo para diagnosticar problemas de replicación relacionados con el análisis de mandatos y la resolución de reglas de replicación de espacio de archivos.
REPLFS	Esta clase de rastreo muestra el rastreo relacionado con la iteración de los espacios de archivos para decidir lo que se replicará, actualizará o suprimirá.	Utilice esta clase de rastreo para diagnosticar los problemas de replicación con los espacios de archivos en iteración para decidir lo que se replicará, actualizará o suprimirá.
REPLINV	Esta clase de rastreo muestra el rastreo relacionado con las actualizaciones de inventario (tablas IM) como parte de la replicación.	Utilice esta clase de rastreo para diagnosticar problemas de replicación con las actualizaciones de inventario.
REPLPROC	Esta clase de rastreo muestra el rastreo del proceso de replicación general. Esta clase de rastreo es la hebra principal y el asignador.	Utilice esta clase de rastreo para diagnosticar problemas de replicación con el proceso de replicación.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
REPLSESS	Esta clase de rastreo muestra el rastreo relacionado con el establecimiento de sesiones para la replicación, incluida la gestión de sesiones en los servidores de origen y de destino.	Utilice esta clase de rastreo para diagnosticar problemas de replicación con el establecimiento de sesiones.
REPLSTATS	Esta clase de rastreo muestra el rastreo relacionado con la actualización de la estadística como ejecuciones de replicación. También incluye la inserción o la actualización de registros del historial en la tabla del historial de replicación.	Utilice esta clase de rastreo para diagnosticar problemas de replicación con las actualizaciones estadísticas.
RETPROT	Clase de rastreo para funciones de protección de retención de copias archivadas.	Utilice esta clase de rastreo para depurar problemas cuando utiliza los parámetros **RETINIT** y **RETMIN** en el grupo de copia de archivo. También puede utilizar esta clase de rastreo para solucionar problemas debido al uso del verbo VB_SignalObject (solo soportado por la API del cliente) para señalar un suceso de objeto o para mantener o liberar un objeto. Finalmente, puede utilizar esta clase de rastreo para los problemas que ocurren durante la supresión de los objetos protegidos por retención.
ROWMGR	Rastrea actividades de operaciones basadas en fila. Las operaciones basadas en fila son: • Abreviar • Suprimir • Captar • Captar siguiente • Captar anterior • Insertar • Buscar enlaces • Actualizar	Utilice esta clase de rastreo para rastrear las actividades de operaciones basadas en fila.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
SCHED	Clase de rastreo para funciones de planificador central. Esta clase de rastreo es aplicable tanto para planificaciones clásicas como para planificaciones mejoradas.	Utilice esta clase de rastreo para depurar problemas que se relacionan con mandatos planificados como **DEFINE/UPDATE/QUERY SCHEDULE** o **DEFINE ASSOCIATION**. Utilice también este rastreo para depurar problemas que están relacionados con los procesos de fondo del planificador, como el gestor de planificación y la solicitud de planificación.
SESSION	Esta clase de rastreo muestra información sobre las sesiones conectadas al servidor, incluidos todos los verbos que se envían y reciben mediante el servidor.	Esta clase de rastreo se recomienda en infracciones de protocolo, errores de proceso de transacciones o en casos en que el cliente se detiene y no responde.
SESSREMOTE	Rastrea la comunicación entre el servidor y el cliente durante las operaciones de copia de seguridad y restauración de NDMP.	Esta clase de rastreo se utiliza para identificar operaciones de copia de seguridad o restauración relacionadas con NDMP que se inician cuando utiliza el cliente de línea de mandatos o web de IBM Spectrum Protect.
SHRED	Esta clase de rastreo muestra información relacionada con las operaciones de destrucción de datos en el servidor.	Esta clase de rastreo se utiliza para diagnosticar problemas de destrucción de datos. Sólo se puede aplicar la destrucción de datos si una o más agrupaciones de almacenamiento del servidor tiene un valor distinto a cero para el atributo SHRED. La actividad relacionada con la destrucción de datos suele producirse principalmente durante los mandatos **EXPIRE INVENTORY**, **DELETE FILESPACE**, **DELETE VOLUME**, **MOVE DATA**, **MIGRATE** y **SHRED DATA**. Otras clases de rastreo que informan de actividad relacionada con la destrucción de datos son BFDESTROY, DFDESTROY, DSALLOC, DSDEALLOC y CRCDATA.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
SPI/SPID	Rastrea la interfaz de protocolo NDMP del servidor.	Las clases de rastreo SPI y SPID se utilizan para identificar problemas relacionados con las operaciones de copia de seguridad o restauración NDMP de los servidores de archivos NAS. Estas clases de rastreo son específicas para las funciones que implementan el protocolo NDMP y se comunican con un servidor de archivos NAS. La clase de rastreo SPID proporciona rastreo más detallado, incluido el rastreo de todos los registros del historial de archivos NDMP que se envían mediante el servidor de archivos NAS.
SSLDATA	Rastreo detallado de la capa de sockets seguros (SSL) utilizado para mostrar información de nivel de byte sobre los datos que se envían o reciben entre el cliente de archivado y copia de seguridad y el servidor.	Utilice la clase de rastreo SSLDATA para depurar los problemas de daños a los datos de la sesión que podrían venir causados por SSL en ejecución mediante las opciones SSLTCP o SSLTCPADMIN. Este rastreo es un rastreo a nivel de byte que puede recopilar una gran cantidad de datos.
SSLINFO	El rastreo SSL general se utiliza para mostrar la configuración y las características de las sesiones SSL entre el cliente de archivado y copia de seguridad y el servidor.	Utilice la clase de rastreo SSLINFO para depurar las conexiones de las sesiones y los errores de reconocimiento que podrían venir causados por SSL en ejecución mediante las opciones de servidor SSLTCP o SSLTCPADMIN. Esta clase de rastreo se puede utilizar en un tándem con las clases de rastreo TCPINFO y SESSION.
TBREORG	Esta clase de rastreo recopila información sobre las actividades de reorganización de tabla e índice que inicia el servidor.	Utilice la clase de rastreo TBREORG para depurar la actividad de reorganización iniciada por el servidor.
TBLMGR	Rastrea actividades de operaciones basadas en tabla.	Utilice la clase de rastreo TBLMGR para consultar operaciones basadas en tabla, como registro, apertura y cierre de tablas.

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
TCP	Esta clase de rastreo recopila información sobre TCP/IP utilizada entre el cliente y bien el servidor o el agente de almacenamiento. TCP es una clase de rastreo agregada. Activa TCPINFO y TCPERROR.	Utilice esta clase de rastreo para depurar errores de conexión de sesión o problemas de archivos dañados que podrían estar causados por la red.
TCPDATA	El rastreo TCP/IP detallado se utiliza para mostrar información a nivel de byte sobre los datos que se envían o reciben.	Utilice esta clase de rastreo para depurar problemas de datos de sesión dañados que podrían estar provocados por la red.
TCPINFO	El rastreo de TCP/IP general se utiliza para mostrar la configuración y las características de TCP/IP en el servidor o en el agente de almacenamiento.	Utilice esta clase de rastreo para depurar problemas de datos de sesión dañados que podrían estar provocados por la red.
TEC	Esta clase de rastreo proporciona información sobre sucesos que se envían a un servidor de TEC. Estos sucesos corresponden al receptor de sucesos de TIVOLI.	Para depurar problemas de conexión que genera el registro de sucesos de TEC.
TOC	Esta clase de rastreo se utiliza para la Tabla de componentes Contents (TOC), que se utiliza durante las operaciones NDMP a nivel de archivos. TOC es una clase de rastreo agregada que activa TOCBUILD, TOCLOAD, TOCREAD y TOCUTIL.	Utilice esta clase de rastreo para depurar problemas durante las operaciones NDMP del nivel de archivos, por ejemplo la copia de seguridad de NDMP con el parámetro TOC=YES, o una restauración de NDMP con el parámetro **FILELIST**.
TOCBUILD	Funciones de compilación de tablas de contenido (TOC).	Utilice esta clase de rastreo para depurar problemas durante una copia de seguridad de NDMP con el parámetro **TOC=YES**.
TOCLOAD	Funciones de carga de tabla de contenido (TOC).	Utilice esta clase de rastreo para depurar problemas cuando visualiza los archivos y directorios en la interfaz gráfica de usuario del cliente (GUI).

Tabla 10. Clases de rastreo del agente de almacenamiento o del servidor (continuación)

Clases de rastreo	Descripción	Uso
TOCREAD	Funciones de lectura de tabla de contenido (TOC).	Utilice esta clase de rastreo para depurar problemas durante un mandato **QUERY TOC** o mientras está intentando cargar un TOC para mostrar archivos y directorios en la GUI del cliente.
TOCUTIL	Funciones de programa de utilidad de tabla de contenido (TOC).	Utilice esta clase de rastreo para depurar problemas que están relacionados con la inicialización del componente TOC o la retención TOC.
UNICODE	Esta clase de rastreo muestra información sobre conversiones de página de códigos y operaciones de espacio de archivos Unicode.	Utilice esta clase de rastreo para depurar problemas que están relacionados con problemas de conversión de página o problemas de espacio de archivo Unicode.
XI	Esta clase de rastreo muestra información general para los mandatos **IMPORT** y **EXPORT**.	Utilice esta clase de rastreo para depurar problemas que están relacionados con los mandatos **IMPORT** y **EXPORT**.

Mandatos de visualización para el servidor o el agente de almacenamiento

Los mandatos **SHOW** son mandatos de diagnóstico no admitidos que se utilizan para mostrar información sobre estructuras de control en memoria y otros atributos de tiempo de ejecución. Los mandatos **SHOW** los utilizan el desarrollo y el servicio sólo como herramientas de diagnóstico. Hay varios mandatos **SHOW** para el cliente de copia de seguridad/archivado.

Dependiendo de la información que muestra un mandato **SHOW**, es posible que haya instancias en las que la información cambie o casos en los que podría detenerse la aplicación (el cliente, servidor o agente de almacenamiento). Los mandatos **SHOW** deben utilizarse solo con la recomendación de IBM Software Support. Los mandatos **SHOW** que están incluidos aquí son una parte de los mandatos **SHOW** disponibles.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento

Mandato SHOW	Descripción	Recomendación
AGGREGATE	Muestra información sobre un objeto agregado en la jerarquía del almacenamiento del servidor. La sintaxis es **SHOW AGGRegate aggr***ID_más_significativo* aggr*ID_menos_significativo*. aggr*ID-high* y aggr*ID-low* son las palabras de 32 bits más significativas y menos significativas del ID agregado de 64 bits del agregado que se consulta.	Emita este mandato para determinar la existencia y los archivos lógicos almacenados en un objeto de agregación en la jerarquía de almacenamiento del servidor. Para los archivos que forman parte del agregado se visualizan el desplazamiento, la longitud y el estado activo de los archivos de copia de seguridad. Si tiene problemas al restaurar o recuperar archivos, dar caducidad o traslado de datos, la copia de seguridad de las agrupaciones de almacenamiento primarias, copiar datos activos de las agrupaciones de datos activos o auditar volúmenes, puede emitir este mandato.
ASQUEUED	Muestra la cola del punto de montaje. La sintaxis es **SHOW ASQueued**.	Para utilizar una unidad, una sesión de cliente o un proceso de servidor, primero debe obtener un punto de montaje. La gestión de puntos de montaje del servidor permite colocar en la cola las sesiones o procesos que están a la espera de obtener puntos de montaje en caso de que se necesiten más puntos de montaje de los que están disponibles. Este mandato es útil para determinar el estado de una solicitud de punto de montaje, especialmente si se ha detenido una sesión o un proceso para un punto de montaje.
ASVOL	Muestra los volúmenes asignados. La sintaxis es **SHOW ASVol**.	A medida que se asignan volúmenes de medios secuenciales para que los utilicen una sesión o un proceso, se realiza un seguimiento de éstos en una lista en memoria. Puede ver esta lista para determinar el estado de los volúmenes en uso así como las situaciones en las que un procesose ha interrumpido o se ha producido un punto muerto o en las que una sesión o proceso parece haber quedado bloqueado o a la espera de un volumen o de algo más.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
BFOBJECT	Muestra la siguiente información en los datos de jerarquía de almacenamiento del servidor: • El estado activo/inactivo de los archivos lógicos dentro de un agregado • El desplazamiento/ longitud de los archivos lógicos dentro de un agregado • El estado activo o el ID de bitfile de propietario de los archivos lógicos dentro de un agregado • El ID de bitfile del enlace si la extensión desduplicada está vinculada a otra extensión La sintaxis es **SHOW BFObject**.	Este mandato le ayuda a determinar la existencia y los atributos de un objeto bitfile en la jerarquía de almacenamiento del servidor. Si tienes problemas para restaurar, recuperar, dar caducidad o auditar un objeto puede emitir este mandato.
CMD DEDUPDELETEINFO	Muestra el estado de las hebras de supresión de segundo plano para los objetos deduplicados dereferenciados.	Emita este mandato para comprobar el estado del proceso de supresión de segundo plano para objetos deduplicados. Cuando se suprima un archivo o se mueva fuera de una agrupación de almacenamiento deduplicada, la extensión se pondrá en cola con un procesador de segundo plano para intentar la eliminación desde la agrupación de almacenamiento. Este mandato es útil para comprobar el retraso de la extensión en cola y del estado de cada hebra de supresión.
CONFIGURATION	El mandato **CONFIGURATION** es un mandato SHOW de resumen que emite de hecho muchos mandatos y consultas show distintos. La sintaxis es **SHOW CONFIGuration**.	Emita este mandato para facilitar una configuración general y otra información sobre el servidor al servicio técnico de IBM.
DB2CONNECTIONS	El mandato DB2CONNECTIONS muestra las conexiones de DB2 definidas procedentes de las diferentes agrupaciones de conexiones. Este mandato no necesita ningún parámetro adicional. La sintaxis es **SHOW DB2CONnections**.	Emita este mandato para mostrar cuántas conexiones de DB2 se han definido, están en uso y libres en total y dentro de una agrupación determinada.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
DB2TABLES	El mandato DB2TABLES muestra las tablas registradas y sus atributos de columna. Este mandato no necesita ningún parámetro adicional. La sintaxis es **SHOW DB2TABles**.	Emita este mandato para mostrar las tabas registradas y sus atributos de columna.
DBVARS	Muestra los atributos globales de la base de datos. La sintaxis es **SHOW DBVars**.	Emita este mandato para ver el estado y los atributos actuales de la base de datos del servidor.
DEDUPOBJECT	Muestra la información sobre deduplicación de datos para los archivos. Cuando emita este mandato, deberá especificar el parámetro **objectID**. Emita el mandato **SHOW VERSION** para determinar el valor de este parámetro. La sintaxis es **SHOW DEDUPObject**.	Emita este mandato para mostrar la información de desduplicación de datos, por ejemplo: • El ID de archivo de bits para cada extensión • El ID de archivo de bits propietario • El desplazamiento y longitud del archivo de bits propietario • El tipo de resumen y el valor del objeto de desduplicación de datos
DEVCLASS	Muestra la información sobre las clases de dispositivo. La sintaxis de este mandato es **SHOW DEVCLass**.	Emita este mandato para mostrar los estados de las unidades asignadas, los atributos de clases de dispositivo y otras informaciones. Con frecuencia este mandato se utiliza para diagnosticar problemas relacionados con los dispositivos o con bloqueos que se han producido mientras se estaba a la espera de una unidad, biblioteca o volumen. El mandato **SHOW LIBRARY** también facilita información complementaria sobre unidades y bibliotecas.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
GROUPLEADERS	Muestra todos los líderes de grupo de copia de seguridad para un objeto del inventario del servidor. La sintaxis es **SHOW GROUPLeaders** *ID_objeto_más_significativo ID_objeto_menos_significativo*. *objID-high* y *objID-low* son las palabras de 32 bits más sinificativas y menos significativas del ID de objeto agregado de 64 bits del objeto que se consulta. La palabra más significativa es opcional; si no se especifica, se da por supuesto el valor cero. El objeto debe ser un objeto de copia de seguridad.	Emita este mandato para determinar las relaciones del grupo de copia de seguridad de un objeto en el inventario del servidor. Si tienes problemas para restaurar, recuperar, dar caducidad o auditar un objeto puede emitir este mandato.
GROUPMEMBERS	Muestra todos los miembros de grupo de copia de seguridad para un objeto del inventario del servidor. La sintaxis es **SHOW GROUPMembers** *ID_objeto_más_significativo ID_objeto_menos_significativo*. *objID-high* y *objID-low* son las palabras de 32 bits más sinificativas y menos significativas del ID de objeto agregado de 64 bits del objeto que se consulta. La palabra más significativa es opcional; si no se especifica, se da por supuesto el valor cero. El objeto debe ser un objeto de copia de seguridad.	Emita este mandato para determinar las relaciones del grupo de copia de seguridad de un objeto en el inventario del servidor. Si tienes problemas para restaurar, recuperar, dar caducidad o auditar un objeto puede emitir este mandato.
INVOBJECT	Muestra información sobre un objeto de inventario en el servidor. La sintaxis es **SHOW INVObject** *ID_objeto_más_significativo ID_objeto_menos_significativo*. *objID-high* y *objID-low* son las palabras de 32 bits más sinificativas y menos significativas del ID de objeto agregado de 64 bits del objeto que se consulta. La palabra más significativa es opcional; si no se especifica, se da por supuesto el valor cero. El objeto puede ser un objeto de copia de seguridad, un objeto de archivado, un objeto gestionado por espacio, etc.	Emita este mandato para determinar la existencia y los atributos de un objeto en el inventario del servidor. Puede emitir este mandato si experimenta problemas al restaurar, recuperar, dar caducidad o auditar el objeto. El mandato **INVOBJECT** notifica los siguientes elementos: • Nueva información para los objetos protegidos con retención de archivado. • Si el objeto de archivado se encuentra en espera de supresión. • Si el objeto utiliza retención basada en eventos.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
LIBINVENTORY	Muestra el estado actual del inventario de biblioteca para la biblioteca especificada. La sintaxis es **SHOW LIBINVentory** *nombre_de_biblioteca*, donde *nombre_de_biblioteca* es opcional de modo que, si no se especifica, el mandato devuelve la información de inventario de todas las bibliotecas.	Emita este mandato si hay un problema con la información de inventario de la biblioteca. El mandato muestra las propiedades de la memoria actual del inventario de biblioteca.
LIBRARY	Utilice el mandato **LIBRARY** para mostrar el estado actual de la biblioteca especificada y todas sus unidades. La sintaxis es **SHOW LIBRary** *nombre_de_biblioteca* donde *nombre_de_biblioteca* es opcional. Si se deja en blanco, el mandato devuelve información para todas las bibliotecas.	Este mandato es útil para obtener una vista rápida de toda la información en memoria relacionada con una biblioteca y sus unidades. Esta salida se puede recopilar para cualquier problema relacionado con las bibliotecas o las unidades, por ejemplo, problemas de montaje.
LOCK	Muestra los poseedores de bloqueo y los elementos en espera. La sintaxis es **SHOW LOCK**.	El servidor y el agente de almacenamiento utilizan bloqueos como mecanismo para serializar el acceso y la actualización de la información y otras construcciones. Esta información se utiliza para diagnosticar las detenciones u otros problemas relacionados con la contención de recursos.
MEMTREND	El mandato **MEMTREND** informa sobre la memoria que utiliza el servidor, en megabytes. Se guarda en intervalos de horas para las últimas 50 horas. Este mandato se ajusta en el código del servidor. No se puede configurar. El mandato también muestra un histograma como ayuda para visualizar la tendencia de utilización. La sintaxis es **SHOW MEMTREnd**.	Emita este mandato para determinar si el servidor tiene una fuga de memoria. Si el uso de la memoria aumenta constantemente, es posible que exista una fuga. Para que las medidas sean válidas, el periodo de medida (las últimas 50 horas) debe ser normal y representar una actividad del servidor regular. La utilización de la que se informa representa la cantidad de memoria que las rutinas internas del servidor solicitan de las rutinas de memoria del pseudokernel. NO representa la cantidad total de memoria que el servidor utiliza. Este mandato ayuda a determinar la tendencia de uso de memoria del servidor.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
MP	Muestra los puntos de montaje. La sintaxis es **SHOW MP**.	Emita este mandato para determinar el volumen que está utilizando un determinado punto de montaje y otros atributos para los puntos de montaje asignados. **SHOW LIBRARY** y **SHOW DEVCLASS** tienen información complementaria útil con este mandato para mostrar el estado actual de las unidades y los recuentos de puntos de montaje devclass actuales.
NASDEV	Muestra los dispositivos SCSI que están adjuntos al archivo de almacenamiento adjunto de red(NAS) asociado con una definición de transporte de datos NAS. La sintaxis es **SHOW NASDev**.	Cree una conexión NDMP (Network Data Management Protocol) con el servidor de archivos NAS especificado y muestre los dispositivos SCSI conectados en el servidor de archivos. Este mandato necesita unicamente un nodo NAS y una definición de transporte de datos.
NASFS	Muestra los sistemas de archivos de un servidor de archivos NAS asociado con una definición de traspaso de datos de NAS. La sintaxis es **SHOW NASFs**.	Cree una conexión NDMP con el servidor de archivos NAS especificado y muestre los sistemas de archivos que se han definido en el servidor de archivos. Se debe realizar una copia de seguridad de cualquier archivo que muestre IBM Spectrum Protect. Este mandato necesita unicamente un nodo NAS y una definición de transporte de datos.
NASINFORMATION	Muestra la información de configuración sobre el servidor de archivos NAS asociado con una definición de traspaso de datos NAS. La sintaxis es **SHOW NASInformation**.	Cree una conexión NDMP para el servidor de archivos NAS especificado y muestre la información general que se recupera del servidor de archivos. Este mandato es útil para identificar problemas de comunicación básicos relacionados con los servidores de archivos NAS, como los errores de autenticación. Este mandato necesita unicamente un nodo NAS y una definición de transporte de datos.
NASWORKLOAD	Muestra la carga de trabajo de los archivos NAS que se utilizan para todas las operaciones de IBM Spectrum Protect. La sintaxis es **SHOW NASWorkload**.	Emite este mandato para determinar la carga de trabajo de traspaso de datos de fondo y las operaciones de restauración y copia de seguridad.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
REPLICATION	Muestra todos los servidores de réplica conocidos y su identificador global único (GUID) así como todos los procesos de réplica en ejecución. Los procesos pueden incluir las estadísticas individuales de cada espacio de archivos y el estado de cada sesión de replicación.	Emita este mandato si la réplica no progresa o si la réplica no funciona correctamente.
RESQUEUE	Muestra la cola de recursos. La sintaxis es **SHOW RESQueue**.	Utilice la cola de recursos para supervisar recursos comunes del servidor. Si un recurso se ha detenido o está en espera durante un tiempo poco razonable, el algoritmo de supervisión del recurso para el servidor cancela el usuario del recurso. Este mandato se utiliza para mostrar información sobre transacciones, bloqueos y otros recursos que utiliza un agente de almacenamiento en el servidor de la base de datos que se va a configurar para utilizarse.
SESSIONS	Muestra información sobre las sesiones que se conectan al servidor o al agente de almacenamiento. La sintaxis es **SHOW SESSions**.	Emita este mandato para diagnosticar interrupciones de sesiones u otros problemas generales relativos a las sesiones mientras una sesión sigue conectada al servidor. Este mandato también es útil en casos en los que se cancela una sesión y sigue mostrándose en **QUERY SESSION**.
SLOTS	Muestra el estado actual de la información de la ranura seleccionada de la biblioteca; por ejemplo, qué volúmenes están en la biblioteca y en qué ranura están. La sintaxis es **SHOW SLOTS** *nombre_biblioteca*.	La información que se muestra es la información que se guarda directamente desde el hardware de la biblioteca a los valores de la memoria. Esta información se puede utilizar para determinar si la información no está sincronizada,es incorrecta o si los valores que devuelve el hardware de la biblioteca no son correctos. De forma alternativa, emita este mandato para determinar los números de los elementos de la unidad para una biblioteca SCSI si **QUERY SAN** no está disponible para una biblioteca determinada.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
SSPOOL	Muestra las agrupaciones de almacenamiento de información. La sintaxis es **SHOW SSPool**.	Emita este mandato para mostrar los estados y atributos de las agrupaciones de almacenamiento definidas.
THREADS	Muestra información sobre todas las hebras conocidas en el servidor. La sintaxis es **SHOW THReads**. **Importante:** En algunos sistemas operativos (como por ejemplo: HP) la información notificada se obtiene sin serialización. En un sistema ocupado, puede que la información no sea coherente, puede que varias hebras informen de que están reteniendo el mismo objeto mútex o puede que una hebra informe de que está a la espera de un objeto mútex que otra hebra que no reclama su retención ha retenido.	El servidor muestra información sobre cada hebra, que normalmente incluye el identificador de hebra de IBM Spectrum Protect, el identificador de hebra del sistema, el nombre de hebra, los objetos Mútex que contiene (si hay alguno) y el objeto Mútex o la condición que espera (si hay alguno). Este mandato es específico de cada plataforma; por lo tanto, puede que la información sea ligeramente distinta entre plataformas. Es posible que desee emitir este mandato si el servidor o un proceso de servidor particular se detiene para que pueda ver si hay hebras esperando a los resultados que mantiene otra hebra.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
TOCSETS	Muestra todos los conjuntos de tabla de contenido (TOC) de los que el servidor tiene constancia. La sintaxis es **SHOW TOCSets DELETE**=*Núm_conjunto* **TOUCH**=*Núm_conjunto*. El parámetro **DELETE** hace que se suprima el número de conjunto de TOC especificado. El parámetro **TOUCH** actualiza la fecha de la última utilización del número de conjunto de TOC especificado. Un conjunto de TOC se retiene durante el periodo de retención TOC que sigue a la última fecha utilizada (consulte el mandato **SET TOCRETENTION**).	Un conjunto de TOC se utiliza durante las operaciones NDMP de archivo. Durante la realización de una copia de seguridad de NDMP con el parámetro TOC=YES, se crea una TOC en la base de datos del servidor. Durante una restauración, puede que se carguen una o varias TOC en la base de datos del servidor para proporcionar los nombres de archivo y de directorio a la GUI del cliente. Este mandato muestra el estado del conjunto de TOC; por ejemplo, si está creándose o cargándose, y la cantidad de espacio temporal de base de datos que está utilizándose para cada conjunto de TOC. Puede emitir este mandato si está experimentando problemas con una copia de seguridad NDMP con el parámetro **TOC=YES**, o si tiene problemas para restaurar los archivos desde una copia de seguridad de NDMP, o si los conjuntos de TOC se retienen en la base de datos del servidor durante demasiado tiempo o muy poco tiempo.
TOCVARS	Muestra la información sobre el componente TOC del servidor. La sintaxis es **SHOW TOCVars**.	Emita este mandato para determinar el estado del componente TOC. Es posible que pueda utilizar este mandato si tiene problemas para completar una copia de seguridad de NDMP con el parámetro **TOC=YES** o si tiene problemas para restaurar los archivos desde una copia de seguridad de NDMP.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
TXNTABLE	Muestra información acerca de las transacciones que están en la lista de utilización del servidor. La sintaxis es **SHOW TXNTable**.	Las transacciones que extrae este mandato las utilizan los procesos de servidor, las sesiones y otras aplicaciones para leer la información de la base de datos, para realizar actualizaciones en la base de datos (como insertar, actualizar o suprimir información) o para gestionar bloqueos. Esta información es útil para diagnosticar los procesos que se han detenido u otros errores relacionados con la transacción mientras la transacción todavía está abierta en el servidor.
VALIDATE LANFREE	Le permite validar si las definiciones están en su sitio en el servidor para que un cliente puede completar operaciones de traslado de datos libres de LAN. En aquellos casos en los que estas definiciones no estén presentes o sean incorrectas, puede que sea difícil determinar si el entorno fuera de la LAN se ha configurado correctamente. La sintaxis es **VALIDATE LANFREE** *nombre_nodo agente_almacenamiento*. **Nota:** El mandato **VALIDATE LANFREE** ha sustituido al mandato **SHOW LANFREE**.	Este mandato evalúa todas las agrupaciones de almacenamiento de destino posibles para este nodo de cliente y notifica si la agrupación de almacenamiento puede albergar operaciones de traspaso de datos fuera de la LAN.
VERSIONS	Emita el mandato **SHOW VERSIONS** para recuperar un **objectID**. El **objectID** es necesario para emitir el mandato **SHOW DEDUPOBJECT**. La sintaxis es **SHOW Versions**.	Emita este mandato para mostrar los ID de objeto.

Tabla 11. Mandatos SHOW del servidor o del agente de almacenamiento (continuación)

Mandato SHOW	Descripción	Recomendación
VOLINUSE	Muestra si el volumen especificado está en lal ista del servidor en uso. El mandato **VOLINUSE** muestra información adicional que puede ser útil, incluido si el volumen está pendiente de eliminación de la lista de en uso. La sintaxis es **SHOW VOLINUSE** *nombre_volumen*. Si es necesario eliminar el volumen de la lista de volúmenes en uso, puede especificar el siguiente parámetro para eliminarlo de la lista: **SHOW VOLINUSE** *nombre_volumen* REMOVE=YES.	Emita este mandato para determinar si un volumen se encuentra en la lista de volúmenes en uso y, en caso necesario, para eliminarlo de esa lista. Las operaciones que se asocian a este volumen puede que no se ejecuten correctamente si el volumen se elimina de la lista de utilización.

Habilitación del rastreo para el controlador de dispositivo de IBM Spectrum Protect

El rastreo está disponible para el controlador de dispositivo de IBM Spectrum Protect. El controlador de dispositivo de IBM Spectrum Protect se puede rastrear desde la consola del servidor, un cliente administrativo o desde un shell que se ejecute en el sistema donde está instalado el controlador de dispositivo.

Las instrucciones de rastreo son aplicables al controlador de dispositivo de IBM Spectrum Protect de todas las plataformas donde se admita el controlador de dispositivo. Para los dispositivos que utilizan controladores de dispositivo diferentes del controlador de dispositivo de IBM Spectrum Protect, la capacidad de rastrear y las instrucciones sobre cómo rastrear esos controladores de dispositivo las proporciona el proveedor del dispositivo.

Referencia relacionada:

"Rastreo desde la consola del servidor"

"Rastreo de datos desde un shell de mandatos de AIX y Windows" en la página 157

Rastreo desde la consola del servidor

Para rastrear el controlador desde el servidor, primero debe emitir los mandatos apropiados.

Emita los mandatos **TRACE ENABLE** y **TRACE BEGIN** para rastrear el controlador desde el servidor.

El controlador de dispositivoIBM Spectrum Protect está formado por dos controladores: uno para dispositivos de cambio automático de biblioteca y uno para dispositivos de cintas. Puede elegir cuál desea rastrear. El mandato tiene la siguiente sintaxis:

DDTRACE START [LIBRARYDD | TAPEDD]
[flags=EE |, FULL |, SYSLOG | BASE]

DDTRACE GET [LIBRARYDD | TAPEDD]
DDTRACE END [LIBRARYDD | TAPEDD]

Las opciones siguientes están disponibles:

START Activa el rastreo y lo graba en un almacenamiento intermedio de la memoria basado en la opción FLAGS predeterminada o especificada.

GET Graba el almacenamiento intermedio de la memoria en el mismo archivo que se especificó con el mandato de servidor **TRACE BEGIN**.

END La detención del rastreo de grabación en el almacenamiento intermedio de la memoria no borra el contenido del almacenamiento intermedio, de modo que puede ejecutarse END antes de ejecutar GET.

LIBRARYDD
Rastrea el controlador de dispositivo que controla los autocambiadores de la biblioteca.

TAPEDD Rastrea el controlador de dispositivo que controla las unidades de cintas.

Para las opciones que se han listado anteriormente, puede especificar cualquier controlador de dispositivo o el controlador de dispositivo de biblioteca y uno de los otros dos. Las opciones y controladores se delimitan por espacios. Por ejemplo:

DDTRACE START TAPEDD - Empieza rastreando el controlador de dispositivo que controla los controladores de cinta.

DDTRACE START LIBRARYDD Empieza rastreando el autocambiador de biblioteca.

DDTRACE START LIBRARYDD TAPEDD Rastrea los controladores de biblioteca y de cinta.

Independientemente de las opciones que utilice, especifique las mismas para todos los mandatos en la serie START-GET-END.

El parámetro **FLAGS** es opcional y no suele ser necesario. Los siguientes valores ser refieren al parámetro **FLAGS**:

EE Rastrea todas las entradas y salidas rutinarias del controlador de dispositivo.

FULL Activa más rastreo de depuración y proporciona más detalles. Dado que el tamaño del almacenamiento intermedio de la memoria es fijo, se rastrea un número inferior de sucesos. No rastrea puntos de entrada y salida rutinarios.

SYSLOG
En algunas plataformas, SYSLOG ordena la grabación de sentencias de rastreo en las anotaciones del sistema además de en el almacenamiento intermedio de la memoria. Esta oferta resulta muy útil al depurar situaciones en las que el kernel se ha detenido o cuando el rastreo se reinicia en el almacenamiento intermedio de la memoria.

BASE BASE es el valor predeterminado y no puede especificarse con otros indicadores. Sólo se utiliza para desactivar los indicadores EE, FULL y SYSLOG sin desactivar el rastreo.

Rastreo de datos desde un shell de mandatos de AIX y Windows

AIX Windows

El programa de utilidad autónomo, ddtrace, imita exactamente los mandatos de servidor **DDTRACE**.

El programa de utilidad ddtrace autónomo está instalado en el directorio de dispositivos, que es el mismo directorio que el de los programas de utilidad mttest, lbtest y optest. Su sintaxis y opciones son idénticas a las del comando de servidor **DDTRACE**. Por ejemplo:

`$ ddtrace start librarydd tapedd flags=EE` - Inicio del rastreo en los controladores de biblioteca y cinta y obtener rastreo de entrada/salida adicional.

`$ ddtrace get librarydd tapedd` - Obtener el rastreo desde memoria y grabarlo en el archivo ddtrace.out.

`$ ddtrace end librarydd tapedd` - Detención del rastreo de memoria.

El uso principal de esta herramienta autónoma es primordialmente para casos en los que el controlador debe rastrearse durante la inicialización del servidor de IBM Spectrum Protect. El programa de utilidad ddtrace graba el almacenamiento intermedio de la memoria en el archivo “ddtrace.out” del directorio activo. Si el archivo existe, se agrega al archivo sin sobrescribirlo.

Rastreo para detectar una anomalía de conversión de página de códigos

El servidor de IBM Spectrum Protect utiliza funciones del sistema operativo para realizar la conversión entre Unicode y la página de códigos del servidor. Si el sistema no se configura correctamente, la conversión falla.

Procedimiento

Siga estos pasos para obtener más información acerca de la anomalía:

1. Comience el rastreo de la clase de rastreo UNICODE.
2. Repita la acción que ha producido el mensaje de error.
3. Consulte el archivo README del servidor para determinar si existe algún requisito específico de la plataforma para la instalación del idioma.
4. Asegúrese de que los entornos nacionales que se indican en las páginas de códigos de problema se han instalado y de que también se han instalado los requisitos que se especifican en el archivo README.

Rastreo de datos para el cliente

Puede activar el rastreo en el cliente o en la interfaz de programas de aplicación (API) de cliente alterando el archivo de opciones de cliente.

Acerca de esta tarea

Realice los siguientes pasos para activar el rastreo en el cliente o en la API del cliente:

Procedimiento

1. Determine las clases de rastreo que desea activar a partir de la tabla siguiente:

Nombre de clase de rastreo	Descripción	Cuándo se utiliza	Notes adicional
SERVICE	Muestra información de proceso general para el cliente.	Es útil en muchos casos. Generalmente, se recomienda en infracciones de protocolo, errores de proceso de transacciones o en casos en que el cliente se detiene y no responde.	
VERBINFO	Recopilar información acerca del protocolo cliente-servidor utilizado porIBM Spectrum Protect.	Para depurar infracciones de protocolo, errores de proceso de transacciones o en los casos en los que el cliente se detiene o no responde.	
VERBDETAIL	Información detallada acerca del protocolo cliente-servidor utilizado por IBM Spectrum Protect. Muestra los almacenamientos intermedios de memoria interna que contienen los verbos enviados y recibidos por el cliente.	Para depurar problemas con datos de sesión dañados que pueden deberse a la red.	Genera una salida de gran tamaño.

2. Active el rastreo añadiendo el texto siguiente al archivo de opciones del cliente: `traceflag <nombre_clase_rastreo>`.

   Atención: *<nombre_clase_rastreo>* puede ser una lista delimitada por comas de clases de rastreo. Por ejemplo, este texto se podría especificar como `traceflag service,verbinfo,verbdetail`.

3. Configure el rastreo para que empiece y emita los mensajes de rastreo a un archivo añadiendo el siguiente texto al archivo de opciones del cliente: `tracefile <nombre_archivo>`.

4. Realice la operación que está causando el problema.

   Consejo: El rastreo también puede configurarse e iniciarse invocando el cliente desde un indicador de mandatos y especificando los indicadores anteriores. Por ejemplo, `dsm -traceflags=service -tracefile=file.out`.

Opciones traceflag del daemon de diario y de registro

Para ejecutar la copia de seguridad con diario, debe utilizar el proceso del daemon de diario. Este proceso sirve para realizar un seguimiento de los cambios en el sistema de archivos y mantener las bases de datos de diario modificadas.

El daemon de diario utiliza el mismo mecanismo de rastreo que el cliente, pero los valores de rastreo se especifican en el archivo de configuración de diario (`tsmjbbd.ini`) como se indica a continuación:

```
[Configuración de diario]
TraceFlags=all_jbb
;
; los dos valores siguientes permiten la segmentación del archivo de rastreo
;
TraceMax=100
TraceSegMax=1
tracefile=tracefiles\trace.out
```

Configuración de rastreo para daemon de diario:

- BTREEDB - Clase básica de base de datos BTREE de nivel inferior
- CACHEDB - Procesamiento de la caché de exclude de Windows 2003
- DBPERF - Rendimiento de operaciones de la base de datos de nivel inferior
- DBSTATS - Rastreo de rendimiento de las operaciones de consulta, inserción/actualización, supresión y recorridos de árbol
- FILEOPS - Actividad de base de datos interna
- JBBCOMM - Hebra a la escucha
- JBBDAEMON - Gestor de procesos
- JBBFILEMON - Monitor de sistema de archivos
- JBBDBACCESS - Hebra de controlador de base de datos
- JBBDBINFO - Acceso a bases de datos de nivel inferior
- JBBNPCOMM - Comunicaciones de Named Pipes
- JBBSERVICE - Rastreo de SERVICE específico de la plataforma Windows
- JBBVERBINFO - Información de verbo detallada
- ALL_JBB - Indicador de rastreo agregado que incluye todos los valores anteriores

Configuración de rastreo del cliente de copia de seguridad/archivado especificado en `dsm.opt`:

- JOURNAL - Rastreo de copia de seguridad basada en el registro por diario

Clases de rastreo de cliente

El cliente proporciona clases de rastreo individuales y agregadas. Las clases de rastreo agregadas son un método abreviado para activar varias clases de rastreo relacionadas especificando simplemente el nombre de la clase de rastreo agregada. Es posible que haya referencias a clases de rastreo que se activan como parte de una clase de rastreo agregada pero que no se describen explícitamente de forma individual.

Las clases de rastreo de Tabla 12 en la página 160 son las clases de rastreo que se solicitan o se utilizan habitualmente para diagnosticar problemas. El nombre de clase de rastreo debe utilizarse con las opciones `TRACEFLAG` en el archivo `dsm.opt`.

Tabla 12. Clases de rastreo

Clase de rastreo	Descripción	Recomendación
ALL_BACK	Muestra la información general del proceso de copia de seguridad para el cliente. Agregación de las clases de rastreo TXN, INCR, POLICY y PFM, e incluidas implícitamente en la clase de rastreo SERVICE.	Utilice esta clase de rastreo para los problemas relacionados con copias de seguridad selectivas o incrementales.
ALL_FILE	Muestra la información general del proceso de copia de seguridad para el cliente. Agregación de las clases de rastreo DIROPS, FILEOPS y FIOATTRIBS, e incluidas implícitamente en la clase de rastreo SERVICE.	Utilice esta clase de rastreo para los problemas relacionados con los datos de lectura y grabación y la obtención de información de atributos de archivo.
ALL_IMAGE	Muestra la información de proceso de imagen para el cliente. Agregación de varias clases de rastreo relacionadas con las imágenes, e incluidas implícitamente en la clase de rastreo SERVICE.	Utilice esta clase de rastreo para los problemas relacionados con todos los aspectos de operaciones de copia de seguridad y restauración de imágenes de volumen.
ALL_JBB	Muestra la información de proceso de copia de seguridad de diario para el cliente. Agregación de varias clases de rastreo con diario relacionadas con las copias de seguridad e incluidas implícitamente en la clase de rastreo SERVICE.	Utilice la clase de rastreo para resolver problemas relacionados con todos los aspectos de las copias de seguridad basadas en diario.
ALL_NAS	Muestra la información de proceso NDMP para el cliente. Agregación de varias clases de rastreo relacionadas con NDMP, e incluidas implícitamente en la clase de rastreo SERVICE.	Utilice esta clase de rastreo para los problemas relacionados con todos los aspectos de operaciones de copia de seguridad y restauración NDMP.
ALL_SESS	Muestra toda la información de verbo y sesión que se envía entre el cliente y el servidor. Agregación de las clases de rastreo SESSION, VERBINFO, SESSVERB, VERBADMIN y VERBDETAIL. Todas las clases de rastreo de esta agregación están incluidas de forma implícita en la clase de rastreo SERVICE, excepto VERBDETAIL.	Utilice esta clase de rastreo para los problemas relacionados con la sesión del cliente y el servidor, tales como el tiempo de espera para la comunicación, infracciones de protocolo y casos en los que el cliente parece estar detenido en espera del servidor, o viceversa.

Tabla 12. Clases de rastreo (continuación)

Clase de rastreo	Descripción	Recomendación
ALL_SNAPSHOT	Muestra información relacionada con las operaciones de instantánea de volumen. Agregación de varias clases de rastreo relacionadas con las instantáneas de volúmenes e incluidas implícitamente en la clase de rastreo SERVICE.	Utilice esta clase de rastreo para determinar los problemas relacionados con instantáneas de volúmenes que se utilizan en operaciones de copia de seguridad de imagen activada y de soporte de archivos abiertos.
ALL_WAS	Muestra información de procesamiento de Web Application Server (WAS) para el cliente. Agregación de varias clases de rastreo relacionadas con WAS e incluidas implícitamente en la clase de rastreo SERVICE.	Utilice esta clase de rastreo para los problemas relacionados con todos los aspectos de operaciones de copia de seguridad y restauración WAS.
AUDIT	Muestra información de auditoría para el proceso de copia de seguridad y restauración. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para conservar un registro de los archivos procesados, validados y restaurados en un archivo.
CLIENTTYPE	Muestra el tipo de cliente en cada línea de la salida del rastreo.	Utilice esta clase de rastreo para rastrear situaciones en las que hay más de un componente de cliente implicado, como la aceptación de clientes y el agente del sistema de archivos.
COMPRESS	Muestra la información de compresión. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para determinar la cantidad de datos que se comprimen según el archivo.
DELTA	Muestra la información de proceso de copia de seguridad de subarchivos adaptable. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para determinar los errores en operaciones de copia de seguridad y restauración de subarchivos adaptable.
DIROPS	Muestra las operaciones de grabación y lectura de directorios. Parte de las agregaciones de rastreo SERVICE y ALL_FILE.	Utilice esta clase de rastreo cuando se produzcan problemas en un directorio de grabación o lectura.
DOMAIN	Muestra la información de proceso de dominio incremental. Parte de las agregaciones de rastreo SERVICE.	Utilice esta clase de rastreo para determinar cómo las sentencias DOMAIN se resuelven durante el proceso de copia de seguridad, como problemas en la resolución del dominio ALL-LOCAL.

Tabla 12. Clases de rastreo (continuación)

Clase de rastreo	Descripción	Recomendación
ENCRYPT	Muestra la información de cifrado de datos. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para determinar si un archivo se incluye en el proceso de cifrado.
ERROR	Muestra la información de errores específicos del sistema operativo. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para determinar el contenido de los verbos enviados entre el cliente y el servidor.
FILEOPS	Muestra las operaciones de lectura y grabación de archivos. Parte de las agregaciones de rastreo SERVICE y ALL_FILE.	Utilice esta clase de rastreo cuando se produzcan problemas en las operaciones de apertura, lectura, grabación o cierre de un archivo.
FIOATTRIBS	Muestra comparaciones de atributos de archivos entre la versión del cliente local y la versión activa en el servidor. Parte de las agregaciones de rastreo SERVICE, ALL_BACK y ALL_FILE.	Utilice esta clase de rastreo al determinar por qué se ha realizado una copia de seguridad de un archivo durante una copia de seguridad incremental.
INCR	Muestra comparaciones de proceso de lista incremental entre el cliente y el servidor. Parte de las agregaciones de rastreo SERVICE y ALL_BACK.	Utilice esta clase de rastreo para determinar si los archivos son candidatos para la copia de seguridad incremental, especialmente junto con la clase de rastreo FIOATTRIBS.
INCLEXCL	Muestra el estado de inclusión o exclusión para los datos que se están procesando. Este indicador también se utiliza para la función de previsualización.	Utilice esta clase de rastreo para determinar qué objeto (generalmente archivo o directorio) se incluye o excluye durante la previsualización o copia de seguridad/archivado.
MEMORY	Muestra las peticiones de asignación y liberación de memoria. Esta clase de rastreo graba una gran cantidad de información en el archivo de rastreo y no se incluye en ninguna clase agregada.	Utilice esta clase de rastreo para determinar fugas de memoria, incrementos de memoria y otros problemas relacionados con la misma.
OPTIONS	Muestra las opciones de proceso actuales. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para determinar qué opciones están en efecto para la sesión actual, y para los problemas al aceptar las opciones de proceso desde los conjuntos de opciones y cliente del servidor.

Tabla 12. Clases de rastreo (continuación)

Clase de rastreo	Descripción	Recomendación
PASSWORD	Muestra la información de acceso de archivo con contraseña (no muestra contraseñas). Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para determinar problemas al leer las contraseñas del servidor desde el almacenamiento local, por ejemplo los errores PASSWORDACCESS= GENERATE.
PID	Muestra el ID de proceso de cada sentencia de rastreo. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para realizar el diagnóstico de problemas que pueden incluir múltiples procesos.
POLICY	Muestra la información de política disponible para el cliente de copia de seguridad/archivado. Parte de las agregaciones de rastreo SERVICE y ALL_BACK.	Utilice esta clase de rastreo para ver las políticas disponibles durante una operación de copia de seguridad o archivado.
SCHEDULER	Muestra la información general de proceso para el planificador. Un agregado que incluye la mayoría de las clases de rastreo de cliente que se listan en esta tabla. Agregación de todas las clases de rastreo excepto MEMORY, THREAD_STATUS y *DETAIL.	Es útil en muchos casos. Esta clase de rastreo generalmente se utiliza para realizar el diagnóstico de problemas del planificador cuando se desconoce la naturaleza del problema. Si se utiliza el indicador de rastreo SCHEDULER, por lo general no es necesario especificar ningún otro indicador de rastreo porque éste ya incluye la mayoría de las clases de rastreo básicas.
SERVICE	Muestra la información general de proceso para el cliente. Un agregado que incluye la mayoría de las clases de rastreo de cliente que se listan en esta tabla. Es un agregado de todas las clases de rastreo excepto las clases MEMORY y *DETAIL. El indicador de rastreo SERVICE puede generar una cantidad considerable de información. Considere la posibilidad de utilizar la opción TRACEMAX con el distintivo de rastreo SERVICE.	Es útil en muchos casos. Esta clase de rastreo generalmente se utiliza cuando se desconoce la naturaleza del problema. Si se utiliza el indicador de rastreo SERVICE, no es necesario especificar ningún otro indicador de rastreo porque éste ya incluye la mayoría de las clases de rastreo básicas.

Tabla 12. Clases de rastreo (continuación)

Clase de rastreo	Descripción	Recomendación
SESSION	Muestra la información mínima de sesión entre el cliente y el servidor. Parte de las agregaciones de rastreo SERVICE y ALL_SESS.	Utilice esta clase de rastreo para otorgar contexto de sesión a errores generales de proceso o con una de las clases de rastreo VERB*, para determinar problemas con la sesión, como tiempo de espera excedido de sesión e infracciones de protocolo.
SESSVERB	Muestra información adicional de sesión entre el cliente y el servidor. Parte de las agregaciones de rastreo SERVICE y ALL_SESS.	Utilice esta clase de rastreo para otorgar contexto de sesión a errores generales de proceso o con una de las clases de rastreo VERB*, para determinar problemas con la sesión, como tiempo de espera excedido de sesión e infracciones de protocolo.
STATS	Muestra estadísticas finales de proceso en el archivo de rastreo. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo para reunir estadísticas finales de proceso en un archivo.
THREAD_STATUS	Muestra el estado de las hebras. Parte de la agregación de rastreo SERVICE.	Utilice esta clase de rastreo al realizar el diagnóstico de problemas relacionados con las hebras.
TXN	Muestra la información de proceso de transacción. Parte de las agregaciones de rastreo SERVICE y ALL_BACK.	Utilice esta clase de rastreo al realizar el diagnóstico de problemas relacionados con los problemas de proceso de transacciones en el servidor, y para problemas tales como reintentos y detenciones de la transacción.
VERBDETAIL	Muestra información detallada de verbo asociada a las sesiones cliente-servidor. Parte de las agregaciones de rastreo ALL_SESS.	Utilice esta clase de rastreo para determinar el contenido de los verbos enviados entre el cliente y el servidor.
VERBINFO	Muestra información de verbo asociada a las sesiones cliente-servidor. Parte de las agregaciones de rastreo SERVICE y ALL_SESS.	Utilice esta clase de rastreo con la opción traceflag SESSION para proporcionar contexto de sesión a los errores de procesamiento generales o para determinar problemas como fin de tiempo de espera de sesión e infracciones de protocolos.

Tabla 12. Clases de rastreo (continuación)

Clase de rastreo	Descripción	Recomendación
WIN2K	Muestra el procesamiento del objeto del sistema o el estado del sistema de Windows. Parte de las agregaciones de rastreo SERVICE. Sólo válido para el cliente de copia de seguridad/archivado de Windows.	Utilice esta clase de rastreo para determinar los errores con las copias de seguridad o restauración de la información del estado del sistema.

Habilitación del rastreo de cliente de archivado y copia de seguridad

Hay dos métodos de rastreo disponibles para el cliente de archivado y copia de seguridad.

El primer método consiste en configurar los parámetros de rastreo antes de iniciar el cliente de archivado y copia de seguridad. El segundo consiste en activar el rastreo mientras se ejecuta el cliente. Seleccione el método de rastreo que desea activar.

Habilitar un rastreo de cliente mediante la línea de mandatos

Puede rastrear el cliente de archivado y copia de seguridad habilitando el rastreo de cliente en la línea de mandatos.

Acerca de esta tarea

Complete los siguientes pasos para activar el rastreo de cliente en la línea de mandatos:

Procedimiento

1. Determine las clases de rastreo que desea activar.
2. Seleccione qué clases de rastreo se habilitarán agregando el texto siguiente al archivo de opciones del cliente `dsm.opt`: `traceflags <nombre_clase_rastreo>`
3. Utilice un signo menos (-) delante de una clase de rastreo para desactivar el rastreo para una clase de rastreo. Asegúrese de que las clases de rastreo desactivadas aparecen al final de la lista de clases de rastreo. Por ejemplo, si desea recopilar un rastreo SERVICE sin las clases SESSION o SESSVERB, especifique el siguiente texto:

   Correcto: `traceflags service,-session,-sessverb`

   Incorrecto: `traceflags -session,-sessverb,service`

   Atención: *<nombre_clase_rastreo>* puede ser una lista delimitada por comas de clases de rastreo. Por ejemplo, este texto se puede introducir como `traceflags service,verbdetail`
4. Seleccione la ubicación de la salida de los mensajes de rastreo añadiendo el siguiente texto al archivo de opciones del cliente: `tracefile <nombre_archivo>`.

   El nombre *tracefile* debe ser completo, por ejemplo:

   Windows `tracefile c:\service\trace.out`

   AIX Linux `tracefile /home/spike/trace.out`

   Mac OS X `tracefile trace.txt`

5. Establezca un tamaño máximo para el archivo de rastreo entre 1 y 4.294.967.295 MB especificando la variable siguiente en el archivo de opciones de cliente: `tracemax <tamaño_ en_mb>`

   Si se especifica un valor máximo, el cliente empezará a grabar información desde el principio del archivo de rastreo (es decir, se reiniciará o acomodará) cuando el rastreo alcance el tamaño máximo. Esta información puede resultar útil al intentar capturar un evento que tenga lugar al final de un proceso de larga duración. Por ejemplo, para especificar un tamaño de archivo de rastreo máximo de 10 MB: `tracemax 10` Cuando el archivo de rastreo alcanza el límite que se especifica con tracemax, "Continúa al principio del archivo" se escribe al final del archivo de rastreo y el rastreo continúa desde la parte superior del archivo. El final del archivo de registro se indica mediante "FIN DE DATOS." Se puede localizar el final del rastreo mediante una búsqueda de esta serie. Si se especifica un tamaño TRACEMAX de 1001 o superior y no se especifica TRACESEGSIZE, el archivo de rastreo se dividirá automáticamente en segmentos múltiples de 1000 MB por segmento (consulte la explicación sobre TRACESEGSIZE).

   Puede elegir dejar que el cliente divida el rastreo en segmentos más pequeños (entre 1 y 1.000 MB por segmento) especificando la siguiente variable en el archivo de opciones de cliente: `tracesegsize <tamaño_segmento_rastreo_en_MB>`

   cuando divide el rastreo en segmentos pequeños, puede gestionar más fácilmente grandes cantidades de datos de rastreo, lo que evita los problemas relacionados con la compresión de archivos de gran tamaño y elimina la necesidad de utilizar un programa de utilidad aparte de "división de archivos". Por ejemplo, emita el siguiente mandato para especificar un tamaño de segmento de rastreo de 200 MB: `tracesegize 200`

   Un nombre de segmento de un archivo de trazo se especifica con la opción tracefile, además de una extensión que indica el número de segmento. Por ejemplo, si especifica `tracefile tsmtrace.out` y `tracesegsize 200`, el rastreo se segmentará en múltiples archivos separados de tamaño inferior a 200 MB cada uno, con los nombres de archivo `tsmtrace.out.1`, `tsmtrace.out.2`, etc. Cuando se especifica el tamaño de los segmentos no deben usarse comas:

   Correcto: `tracemax 1000`

   Incorrecto: `tracemax 1,000`

   Si utiliza la opción `TRACESEGSIZE`, los segmentos del archivo de rastreo se denominarán mediante el nombre especificado en el archivo de opciones con una extensión adicional que utiliza el número de segmento. Por ejemplo, `trace.out.1`
6. Realice la operación que causa el problema.

Qué hacer a continuación

El rastreo también puede configurarse e iniciarse invocando el cliente desde un indicador de mandatos y especificando los indicadores definidos anteriormente. Por ejemplo:

```
dsmc -traceflags=service,verbdetail -tracefile=tsmtrace.out
-tracemax=2500 -tracesegsize=200
```

Referencia relacionada:

"Clases de rastreo de cliente" en la página 159

Habilitación del rastreo mientras se ejecuta el cliente

Puede rastrear el cliente de archivado y copia de seguridad disponible mientras se ejecuta el cliente.

Antes de empezar

- El cliente de archivado y copia de seguridad debe estar instalado para poder utilizar rastreo dinámico.
- La opción `DSMTRACELISTEN YES` debe estar en vigor cuando se inicie el cliente.
  - AIX Linux Esta opción se especifica en el archivo de opciones del sistema (`dsm.sys`) en la stanza que utiliza el cliente. Para utilizar dsmtrace los usuarios debe iniciar sesión como root.
  - Windows Esta opción se especifica en el archivo de opciones de cliente (normalmente `dsm.opt`). Los usuarios deben iniciar sesión como miembros del grupo de Administradores.

Cuando el cliente se inicia, comienza una hebra de "escucha de rastreo" independiente. Esta hebra "escucha" en un conducto con nombre, a la espera de ser contactada por el programa de utilidad dsmtrace. Para que el nombre del conducto con nombre sea exclusivo, el ID de proceso (PID) del cliente forma parte de dicho nombre. Cuando utiliza dsmtrace para configurar el rastreo, contacta con el cliente a través del conducto con nombre donde el cliente escucha y le pasa la operación de configuración de rastreo preferida. Entonces el cliente pasa los resultados de la operación a dsmtrace a través de otro conducto de salida de nombre similar. dsmtrace muestra los resultados a la consola. El cliente sólo inicia la hebra de escucha de rastreo cuando la opción de cliente `DSMTRACELISTEN YES` está en vigor. Si `DSMTRACELISTEN NO` está en vigor, la hebra de escucha no se inicia y el rastreo dinámico no está disponible para ese cliente. `DSMTRACELISTEN NO` es el valor predeterminado.

Acerca de esta tarea

Los pasos para recopilar un rastreo de cliente son los siguientes:

Procedimiento

1. Detenga el cliente de archivado y copia de seguridad.
2. Configure el archivo de opciones de cliente con las opciones de rastreo preferidas.
3. Reinicie el cliente de archivado y copia de seguridad y reproduzca el problema.
4. Detenga el cliente de archivado y copia de seguridad.
5. Elimine las opciones de rastreo del archivo de opciones del cliente de archivado y copia de seguridad.
6. Enviar el archivo de rastreo resultante al soporte técnico de IBM para su análisis.

   Puede utilizar el programa de utilidad dsmtrace para iniciar, detener y configurar el rastreo de cliente de forma dinámica sin tener que detener el cliente o modificar el archivo de opciones. El rastreo dinámico es especialmente útil cuando sólo debe que rastrear el inicio de operaciones de cliente de archivado de copia de seguridad de larga duración o cuando debe iniciar el rastreo después de que el cliente de archivado y copia de seguridad se ejecutara durante algún tiempo.

   El programa de utilidad dsmtrace incluye las características siguientes:

   - Identifique los procesos en ejecución y sus ID de proceso (PID)

- Activa el rastreo de cliente.
- Desactiva el rastreo de cliente.
- Consulta el estado del rastreo de cliente.

En la tabla siguiente se resume la disponibilidad de esta característica:

Tabla 13. Disponibilidad del programa de utilidad dsmtrace

Componente de cliente	Nombre del programa AIX o Linux	Nombre del programa de Windows
Cliente de copia de seguridad/archivado (línea de mandatos)	dsmc	`dsmc.exe`
Cliente de copia de seguridad/archivado (GUI)	N/D	`dsmagent.exe`
Aceptación de clientes	dsmcad	`dsmcad.exe`
Agente de cliente remoto	dsmagent	`dsmagent.exe`
Servicio planificador	N/D	`dsmcsvc.exe`
Servicio de diario	N/D	`tsmjbbd.exe`
Data Protection for Domino (línea de mandatos)	domdsmc	`domdsmc.exe`
Data Protection for Domino (GUI)	N/D	`domdsm.exe`
Data Protection for Microsoft Exchange (línea de mandatos)	N/D	`tdpexcc.exe`
Data Protection for Microsoft Exchange (GUI)	N/D	`tdpexc.exe`
Data Protection for Microsoft SQL Server (línea de mandatos)	N/D	`tdpsqlc.exe`
Data Protection for Microsoft SQL Server (GUI)	N/D	`tdpsql.exe`

Nota:

- La columna del centro de Tabla 13 incluye Macintosh OS X.
- El rastreo de componentes de Data Protection sólo se realiza para la interfaz de programación de aplicaciones (API) de IBM Spectrum Protect.
- El rastreo de la API de IBM Spectrum Protect está disponible con cualquier aplicación de múltiples hebras que utilice la API de IBM Spectrum Protect. El nombre del archivo ejecutable es el nombre del programa de aplicación que carga la API.

Ejemplo

El siguiente ejemplo muestra cómo habilitar el rastreo de cliente cuando éste se está ejecutando:

1. Identifique el ID de proceso (PID) del cliente de archivado y copia de seguridad que desea rastrear (asegúrese de que `DSMTRACELISTEN YES` está en vigor). Emita el siguiente mandato para mostrar todas las instancias en ejecución del cliente: `dsmtrace query pids`

   Ejemplo de salida:

```
D:\tsm>dsmtrace query pids

IBM Spectrum Protect
programa de utilidad dsmtrace
 dsmtrace Versión 5, Release 3, Nivel 0.0
 dsmtrace fecha/hora: 10/24/2004 21:07:36
(c) Copyright IBM Corporation y otros 1990, 2004.
Reservados todos los derechos.

PROCESS ID  PROCESS OWNER  DESCRIPTION                   EXECUTABLE NAME
4020        andy           Backup-Archive Client (CLI)   dsmc.exe

D:\tsm>
```

Importante: Linux El modelo de hebras de algunas versiones de Linux es ejecutar cada hebra como proceso separado, lo que significa que cuando se consulta la información de proceso, pueden detectarse varios procesos para cada instancia del cliente. El proceso que tiene que identificar es el proceso padre dsmc. Por ejemplo:

```
fvtlinuxppc:/opt/tivoli/tsm/client/ba/bin # dsmtrace q p

IBM Spectrum Protect
programa de utilidad dsmtrace
 dsmtrace Versión 5, Release 3, Nivel 0.0
 dsmtrace fecha/hora: 10/24/04   08:07:37
(c) Copyright IBM Corporation y otros 1990, 2004. Reservados todos los derechos.

PROCESS ID   PROCESS OWNER  DESCRIPTION                   EXECUTABLE NAME
28970       root           Backup-Archive Client (CLI)    dsmc
28969       root           Backup-Archive Client (CLI)    dsmc
28968       root           Backup-Archive Client (CLI)    dsmc
28967       root           Backup-Archive Client (CLI)    dsmc

fvtlinuxppc:/opt/tivoli/tsm/client/ba/bin #
```

En tal caso, emita el mandato **PS** para identificar el proceso padre dsmc:

```
linuxppc:~ # ps -ef | grep dsmc

root   28967   1151   0    Oct22 pts/16   00:00:00  dsmc
root   28968   28967  0    Oct22 pts/16   00:00:00  dsmc
root   28969   28968  0    Oct22 pts/16   00:00:00  dsmc
root   28970   28968  0    Oct22 pts/16   00:00:00  dsmc
root   24092   24076  0    08:15 pts/93   00:00:00   grep dsmc

linuxppc:~ #
```

Tenga en cuenta que el proceso padre de los procesos 28969 y 28970 es el 28968. El proceso padre del proceso 28968 es 28967. El proceso padre del proceso 28967 es 1151, pero el proceso 1151 no aparece en esta salida en pantalla. El proceso 1151 es el proceso que ha iniciado dsmc. Por lo tanto, el ID de proceso padre correcto es 28967.

2. Emita el siguiente mandato para habilitar el rastreo en el cliente:

   ```
   dsmtrace enable 4020 -traceflags=service -tracefile=d:\trace.txt
   ```

   Ejemplo de salida:

   ```
   C:\archivos de programa\tivoli\tsm\baclient>dsmtrace enable 4020
   -traceflags=service
   -tracefile=d:\trace.txt

   IBM Spectrum Protect
   programa de utilidad dsmtrace
    dsmtrace Versión 5, Release 3, Nivel 0.0
   ```

```
 dsmtrace fecha/hora: 10/24/2004 21:45:54
(c) Copyright IBM Corporation y otros 1990, 2004. Reservados todos los derechos.

ANS2805I Se ha activado el rastreo.

C:\archivos de programa\tivoli\tsm\baclient>
C:\archivos de programa\tivoli\tsm\baclient>
```

Importante: Cuando rastree una aplicación de API, debe incluir la opción `-pipenameprefix`.

- AIX Linux Utilice el prefijo `/tmp/TsmTraceTargetAPI`
- Windows Utilice el prefijo `/tmp/TsmTraceTargetAPI`

3. Cuando se han recopilado datos de rastreo suficientes, desactive el rastreo emitiendo el siguiente mandato:

   ```
   dsmtrace disable 4020
   ```

   Ejemplo de salida:

   ```
   C:\archivos de programa\tivoli\tsm\baclient>dsmtrace disable 4020

   IBM Spectrum Protect
   programa de utilidad dsmtrace
     dsmtrace Versión 5, Release 3, Nivel 0.0
     dsmtrace fecha/hora: 10/24/2004 21:47:43
   (c) Copyright IBM Corporation y otros 1990, 2004. Reservados todos los derechos.

   ANS2802I El rastreo está desactivado.
   ```

En la siguiente lista se definen otros ejemplos de habilitación del rastreo de cliente cuando éste se está ejecutando:

dsmtrace query pids
: Este mandato muestra todos los procesos en ejecución cuyos nombres se incluyen en la tabla de la sección Segundo plano.

dsmtrace query pids -filter=*
: Este mandato muestra todos los procesos en ejecución.

dsmtrace query pids -filter=dsm*
: Este mandato muestra todos los procesos en ejecución cuyo nombre empieza por “dsm”

dsmtrace query pids -filter=dsm?
: Esta mandato muestra todos los procesos en ejecución cuyo nombre empieza por “dsm” más otro carácter.

dsmtrace enable 2132 -traceflags=service -tracefile=c:\trace.txt
: Este mandato activa el rastreo de SERVICE para el proceso 2132. La salida del rastreo se graba en el archivo `c:\trace.txt`.

dsmtrace enable 2132 -traceflags=-extrc
: Este mandato desactiva el rastreo de extrc para el proceso 2132 (presumiblemente el rastreo ya se está ejecutando para este proceso).

dsmtrace enable 4978 -traceflags=fileops -tracefile=/tmp/dsmtrace.out -tracemax=1000 -tracesegsize=200
: Este mandato activa el rastreo FILEOPS para el proceso 4978. El rastreo se graba en los archivos `/tmp/dsmtrace.out.1`, `/tmp/dsmtrace.out.2`, etc., y cada archivo no supera los 200 MB. Cuando se han grabado 1000 MB, el rastreo vuelve a almacenarse en `/tmp/dsmtrace.out.1`.

dsmtrace query trace 4978 -on
Este mandato muestra información de rastreo básica y enumera los indicadores de rastreo que están activados para el proceso 4978.

dsmtrace disable 4978
Este mandato inhabilita el rastreo para el proceso 4978.

dsmtrace disable 364 -pipenameprefix=/tmp/TsmTraceTargetAPI
Este mandato inhabilita el rastreo para el proceso 364 de la aplicación de la API.

Problemas y limitaciones conocidos respecto al rastreo

Se han recopilado los problemas y las limitaciones conocidos de procesos de rastreo para ayudarle a resolver problemas que pueda hallar al ejecutar un proceso de rastreo.

- Si el rastreo no está activo actualmente para un proceso y dsmtrace se utiliza sólo con la opción `-TRACEFLAGS`, (por ejemplo, **dsmtrace enable 2346 -traceflags=service**, verá el mensaje siguiente:

  ```
  ANS2805I Se ha activado el rastreo.
  ```

  En este caso, los indicadores de rastreo estaban habilitados, pero es rastreo no está activo hasta que se especifica un archivo de rastreo mediante la opción -TRACEFILE.
- No utilice el comando dsmtrace enable para iniciar el rastreo de la interfaz de programación de aplicaciones (API) para aplicaciones de Data Protection si la aplicación de Data Protection se ejecuta de manera que impide que se conecte al servidor de IBM Spectrum Protect. Por ejemplo, la protección de datos para la interfaz de línea de mandatos IBM Domino tiene varios de estos mandatos:
  - domdsmc help
  - domdsmc set
  - domdsmc query domino
  - domdsmc query pendingdbs
  - domdsmc query preferences

  Si utiliza dsmtrace para habilitar el rastreo de esos mandatos, puede que el proceso de dsmtrace deje de responder y (solo AIX y Linux) que se genere un conducto con nombre residual en el directorio /tmp.
- Windows Para utilizar dsmtrace debe haber iniciado sesión como un administrador local.
- Para utilizar dsmtrace debe haber iniciado sesión como root. Si un proceso de cliente se detiene, éste podrá dejar un conducto con nombre(UNIX FIFO) en el directorio /tmp. Estos FIFO tienen nombres que empiezan por TsmTrace e incluyen un número de ID de proceso (PID). Si un proceso de cliente se detiene o se fuerza su terminación y se inicia otro proceso de cliente cuyo PID coincide con el del FIFO residual anterior, es probable que la hebra de escucha de rastreo no se inicie. Los archivos FIFO antiguos con números de proceso que no coinciden con los archivos FIFO que se ejecutan en los procesos de IBM Spectrum Protect pueden suprimirse con seguridad. NO suprima el FIFO de un proceso en ejecución.
- El modelo de hebras de algunas versiones de Linux es ejecutar cada hebra como proceso separado, lo que significa que cuando se consulta la información de proceso, pueden detectarse varios procesos para cada instancia del cliente. El proceso que tiene que identificar es el proceso padre dsmc.
- Cuando ejecute varias instancias del mismo programa, debe identificar el PID de la instancia que desee rastrear. En esa situación, información como la

información de proceso desde el sistema operativo podría estar disponible para ayudarle a identificar el PID necesario. Por ejemplo, si desea rastrear un dsmc que está ejecutando el usuario 'andy' y hay dos instancias de dsmc, una del usuario 'andy' y otra del usuario 'kevin', puede utilizar al propietario del proceso para identificar qué proceso rastrear.

- Si un archivo de opciones contiene una opción falsa y el cliente no se inicia, es posible que vea algunos errores de dl conducto con nombre en el archivo `dsmerror.log`. Estos mensajes de error se pueden pasar por alto sin ningún problema.

Opciones de rastreo

El rastreo tiene varias opciones que puede utilizar.

DSMTRACEListen

DSMTRACEListen No | Yes

No El cliente no inicia la hebra de escucha de rastreo y el rastreo dinámico no está disponible. El valor predeterminado es No.

Sí El cliente inicia la hebra de escucha de rastreo y el rastreo dinámico está disponible.

Windows La opción `DSMTRACEListen` se especifica en el archivo de opciones del cliente (normalmente `dsm.opt`).

dsmtrace

dsmtrace enable <*pid*> <*opciones*>

Utilice esta mandato para iniciar o modificar el rastreo de un proceso.

pid ID de proceso (PID) del cliente. Utilice dsmtrace query pids o los recursos de su sistema operativo para identificar el PID correcto.

opciones
Opciones de rastreo de cliente.

dsmtrace disable <*pid*>[<*opciones*>]

Utilice este mandato para detener el rastreo de un proceso. El archivo de rastreo se cerrará y los distintivos de rastreo, el tamaño de rastreo máximo, el tamaño de segmento de rastreo máximo y el nombre de archivo de rastreo se borrarán.

<*pid*> El PID para el cliente. Utilice **dsmtrace query pids** o los recursos de su sistema operativo para identificar el PID correcto.

<*opciones*>
Opciones de rastreo de cliente.

dsmtrace help

Este mandato muestra la sintaxis básica de dsmtrace.

dsmtrace query pids [-Filter=<*espec*>**]**

<*espec*>
La especificación del filtro del nombre de proceso del cliente, que puede incluir caracteres comodín “?” (que coincide exactamente con un carácter) o “*” (que coincide con cero o más caracteres).

Si no se especifica ningún filtro, el funcionamiento predeterminado es mostrar la información de proceso de cualquier instancia en ejecución de los nombres de programa que aparecen en la tabla del apartado Historial anterior.

Importante: AIX Linux Cuando utilice la opción FILTER, ponga el símbolo * antes y después del texto de búsqueda. Este ajuste es necesario porque el nombre del archivo ejecutable a menudo incluye la vía de acceso al principio y, en algunos casos, el nombre del archivo ejecutable puede tener más caracteres al final. Por ejemplo:

- `/opt/tivoli/tsm/client/ba/bin/dsmc`
- `domdsmc_DominoUserID`

Por lo tanto, en lugar de -filter=dsmc o -filter=domdsmc, utilice -filter=*dsmc* o -filter=*domdsmc*.

dsmtrace query trace <*pid*> [<*opciones*>] [<*tipo_visualización*>] [-ALl | -ON | -OFf | -BASic]

<pid> ID de proceso (PID) del cliente. Utilice dsmtrace query pids o los recursos de su sistema operativo para identificar el PID correcto.

<opciones>
Opciones de rastreo de cliente.

<tipo_visualización>
El tipo de visualización puede ser una de las siguientes entradas:

ALl Muestra todos los indicadores de rastreo e indica si están activados o desactivados. También se incluye la información que se muestra con el tipo de visualización -BASIC.

ON Muestra los nombres de los indicadores de rastreo que se han activado. También se incluye la información que se muestra con el tipo de visualización -BASIC.

OFf Muestra los nombres de los indicadores de rastreo que se han desactivado. También se incluye la información que se muestra con el tipo de visualización -BASIC.

BASic Muestra el nombre del archivo de rastreo y los tamaños máximos de rastreo y de segmento de rastreo. Este tipo de visualización también indica si el rastreo está activado o desactivado.

-PIPENameprefix

-PIPENameprefix=<*prefijo_nombre_conducto*>
La opción `-PIPENameprefix` debe utilizarse cuando se rastreen aplicaciones de interfaz de programación de aplicaciones (API):

- AIX Linux Utilice el prefijo `/tmp/TsmTraceTargetAPI`
- Windows Utilice el prefijo `/tmp/TsmTraceTargetAPI`

-TRACEFIle

-TRACEFIle=<*nombre_archivo_rastreo*>

La opción -TRACEFIle debe especificar un nombre de archivo válido en el que se debe grabar el rastreo. Si el rastreo ya se está ejecutando, esta opción no tiene ningún efecto.

-TRACEFLags

-TRACEFLags=<*indicadores_rastreo*>

Especifique uno o más indicadores de rastreo. Se suele utilizar el indicador SERVICE. Separe los distintivos de rastreo distintos con una coma. Los indicadores de rastreo también se pueden desactivar incluyendo un prefijo en el nombre del indicador con un signo menos. Cuando combine indicadores de rastreo que desee activar con indicadores de rastreo que desee desactivar, especifique los indicadores que desee desactivar al final de la lista. Por ejemplo, si desea activar el rastreo de SERVICE, excepto para VERBDETAIL, especifique -TRACEFLAGS=SERVICE,-VERBDETAIL. Si el rastreo ya se está ejecutando, esta opción se puede utilizar para activar indicadores de rastreo adicionales o para desactivar indicadores de rastreo.

-TRACEMax

-TRACEMax=<*tamaño_máximo_rastreo*>

Esta opción limita la longitud máxima del archivo de rastreo en el valor especificado (de manera predeterminada, el archivo de rastreo aumenta de forma indefinida). Cuando se alcanza la longitud máxima, el rastreo comienza a incluir datos al principio del archivo. Especifique un valor en MB entre 1 y 4095. Si el rastreo ya se está ejecutando, esta opción no tiene efecto.

-TRACESegsize

-TRACESegsize=<*tamaño_máximo_segmento_rastreo*>

Esta opción se utiliza cuando se prevé disponer de un archivo de rastreo de gran tamaño y desea que el archivo de rastreo se grabe en segmentos más pequeños y fáciles de manejar. Cada segmento no supera el tamaño especificado. Cuando se utiliza esta opción, se añade un número de segmento al nombre del archivo de rastreo para cada segmento. Especifique un valor en MB entre 1 y 1000. Si el rastreo ya se está ejecutando, esta opción no tiene efecto.

Nota:

- Para activar el rastreo para un proceso, debe utilizar las opciones -TRACEFLAGS y -TRACEFILE (y -PIPENAMEPREFIX al rastrear una aplicación de la API).
- Para modificar los indicadores de rastreo para un proceso existente, utilice -TRACEFLAGS (y -PIPENAMEPREFIX al rastrear una aplicación de API).
- Si necesita modificar el nombre del archivo de rastreo, el tamaño máximo de rastreo o el tamaño máximo del segmento de rastreo, necesita primero inhabilitar el rastreo completamente (consulte el mandato **dsmtrace disable**).

Determinar si los datos están cifrados o comprimidos durante la copia de seguridad/restauración a través del rastreo

Debe efectuar diferentes pasos para determinar si durante la copia de seguridad-restauración los datos están comprimidos o cifrados, o ambas opciones.

Procedimiento

1. Añada las opciones de rastreo que aparecen en la lista al archivo de opciones del cliente antes de realizar la copia de seguridad o archivar los objetos:
   - TRACEFILE <*nombre_archivo_rastreo*>
   - TRACEFLAGS api api_detail
2. Examine el archivo de rastreo tras la operación y encuentre una sentencia similar a la siguiente:

   dsmSendObj ENTRY:... objNameP: <*nombre_archivo*>

   Esta salida va seguida del siguiente mensaje de rastreo que indica si el objeto está comprimido, cifrado, o comprimido y cifrado:

   ```
   tsmEndSendObjEx: Total bytes send * *, encryptType is *** encryptAlg is ***
   compress is *, totalCompress is * * totalLFBytesSent * *
   ```

   ```
   +-------------------------------------------------------------------+
   | encryptType/compress | 0 | 1 |
   +-------------------------------------------------------------------+
   | NO | not compressed, not encrypted | compressed, not encrypted |
   | CLIENTENCRKEY | not compressed, encrypted | compressed, encrypted |
   | USER | not compressed, encrypted | compressed, encrypted |
   +-------------------------------------------------------------------+
   ```

   De forma alternativa, su propia aplicación puede determinar el tipo/nivel de cifrado y la compresión de sus datos utilizando la llamada de función **dsmEndSendObjEx** y la estructura de datos **dsmEndSendObjExOut_t**.

   ```
   /*-------------------------------------------------------------------+
   |  Definición de tipo para dsmEndSendObjExOut_t
   +-------------------------------------------------------------------*/
   typedef struct dsmEndSendObjExOut_t
   {
   dsUint16_t         stVersion;        /* structure version */
   dsStruct64_t   totalBytesSent;     /* total bytes read from app */
   dsmBool_t      objCompressed;      /* was object compressed */
   dsStruct64_t   totalCompressSize;  /* total size after compress */
   dsStruct64_t   totalLFBytesSent;   /* total bytes sent LAN Free */
   dsUint8_t      encryptionType;     /* type of encryption used */
   }dsmEndSendObjExOut_t;

   objCompressed  - Indicador que muestra si se ha comprimido el objeto.
   encryptionType - Indicador que muestra el tipo de cifrado.

   Por ejemplo:

     ...
     rc = dsmEndSendObjEx(&endSendObjExIn, &endSendObjExOut);
     if (rc)
     {
     printf("*** dsmEndSendObjEx failed: ");
     rcApiOut(dsmHandle, rc);
   }
   else
   {
    printf("Compression:     %s\n",
    endSendObjExOut.objCompressed == bTrue ? "YES" : "NO");

    printf("Encryption:     %s\n",
    endSendObjExOut.encryptionType & DSM_ENCRYPT_CLIENTENCRKEY ?
   ```

```
"CLIENTENCRKEY" :
endSendObjExOut.encryptionType & DSM_ENCRYPT_USER ? "USER" : "NO");
printf("Encryption Strength: %s\n\n",
endSendObjExOut.encryptionType & DSM_ENCRYPT_AES_256BIT ? "AES_256BIT" :
endSendObjExOut.encryptionType & DSM_ENCRYPT_AES_128BIT ? "AES_128BIT" :
endSendObjExOut.encryptionType & DSM_ENCRYPT_DES_56BIT ? "DES_56BIT" :
 "NONE");
}
...
```

Qué hacer a continuación

Consulte las *Llamadas de función de API* en *Uso de la interfaz de programación de la aplicación* para obtener más información.

Datos de rastreo para la API

Puede activar el rastreo de la interfaz de programas de aplicación (API).

Para activar el rastreo de la API de IBM Spectrum Protect, añada las líneas siguientes al archivo `dsm.opt` o a otro archivo designado como archivo de opciones del cliente:

```
TRACEFILE
nombre_archivo_rastreo
TRACEFLAGS  indicadores_rastreo
```

nombre_archivo_rastreo
El nombre del archivo donde desea grabar los datos de rastreo.

indicadores_rastreo
La lista de indicadores de rastreo para activar. Separe los diferentes indicadores de rastreo mediante un espacio. Los siguientes indicadores de rastreo son específicos de la API de IBM Spectrum Protect:

api Información acerca de las llamadas de función de API

api_detail
Información detallada acerca de las llamadas de función de API

También puede especificar otro cliente de archivo de copia de seguridad e indicadores de rastreo de API de IBM Spectrum Protect. Consulte la documentación de cliente de copia de seguridad/archivado para obtener una lista de las clases de rastreo disponibles. Por ejemplo:

- `TRACEFILE /log/trace.out`
- TRACEFLAGS api api_detail verbinfo verbdetail time stamp

Importante: Si no dispone de permiso de grabación para el archivo indicado por la opción TRACEFILE, dsmSetup o dsmInitEx/dsmInit fallan con un código de retorno DSM_RC_CANNOT_OPEN_TRACEFILE (426).

Para habilitar el rastreo de la API de varias hebras cuando una aplicación se ha iniciado, utilice el programa de utilidad `dsmtrace`. El programa de utilidad `dsmtrace` le permite activar el rastreo mientras se está produciendo el problema, sin tener habilitado el rastreo constantemente. Consulte la sección *dsmtrace*.

Rastreo del agente de Tivoli Monitoring para Tivoli Storage Manager en un sistema AIX o Linux

AIX Linux

Al utilizar Tivoli Monitoring para Tivoli Storage Manager, puede crear y configurar instancias de agentes que supervisen servidores de IBM Spectrum Protect. Detenga todas las instancias del agente, modifique los archivos de configuración y reinicie las instancias del agente para activar el rastreo de agentes de supervisión para los servidores en AIX o Linux.

Acerca de esta tarea

Antes de activar el rastreo, también puede abrir el espacio de trabajo de registro de agente de Tivoli Enterprise Portal y ver las actividades de agente. El espacio de trabajo de Anotaciones del agente contiene información acerca de cualquier servidor de IBM Spectrum Protect que tenga una instancia de agente configurada para supervisarlo. Puede ver la salida del archivo de rastreo sin tener que activar el archivo de rastreo utilizando el grupo de atributo del Registro de agentes.

Realice los pasos siguientes para activar el rastreo:

Procedimiento

1. Desde una ventana de mandatos, vaya al directorio siguiente:
   ```
   cd install_dir/itm/bin
   ```
   donde *install_dir* es el directorio de instalación del agente de supervisión. El directorio de instalación predeterminado es `/opt/tivoli/tsm/reporting`. Si ha instalado el agente de supervisión en el servidor de IBM Tivoli Monitoring existente, vaya al directorio `bin`. El directorio de instalación predeterminado es `/opt/IBM/ITM`.
2. Detenga las instancias del agente de supervisión completando uno de los pasos siguientes:
   - Detenga los agentes de supervisión utilizando la interfaz gráfica de usuario CandleManage emitiendo los mandatos siguientes:
     a. Ejecute el programa CandleManage emitiendo los siguientes mandatos:
        ```
        ./CandleManage &
        ```
     b. En la ventana Manage Tivoli Enterprise Monitoring Services, verifique que el agente de supervisión se ha detenido. Si no se ha detenido, seleccione la instancia de agente aplicable, pulse el botón derecho sobre ella y seleccione **Detener**.
   - Detenga los agentes de supervisión desde la línea de mandatos emitiendo los mandatos siguientes:
     a. `./itmcmd agent -o nombre_instancia stop sk`
3. Para asegurarse de que todos los agentes están detenidos, realice los pasos siguientes:
   a. Espere hasta que la interfaz gráfica de CandleManage informe de que el agente se ha detenido.
   b. Verifique si el proceso siguiente se está ejecutando emitiendo el mandato siguiente:
      ```
      ps -ef | grep -i SK
      ```

c. Si el proceso se está ejecutando, detenga el proceso emitiendo el mandato siguiente:

   ```
   kill -9 ID_proceso
   ```

4. Ubique el directorio donde se almacenan los archivos de configuración emitiendo el mandato siguiente:

   ```
   dir_instalación/itm/config
   ```

5. Para activar el rastreo de agente de supervisión, asegúrese de que el siguiente valor esté establecido en el archivo `sk_agentInstance.config`:

   ```
   KSK_TRACE='1'
   ```

   Debe también asegurarse de que está establecido el valor siguiente en el archivo de configuración `sk.ini`:

   ```
   KSK_TRACE=1
   ```

6. Si un representante de soporte de IBM le pide que active el rastreo para la API, asegúrese de que está establecido el siguiente valor en el archivo `sk_agentInstance.config`:

   ```
   KSK_APITRACE='1'
   ```

   Debe también asegurarse de que está establecido el valor siguiente en el archivo de configuración `sk.ini`:

   ```
   KSK_APITRACE=1
   ```

7. Inicie las instancias del agente de Tivoli Monitoring para Tivoli Storage Manager completando uno de los pasos siguientes:
   - Desde la línea de mandatos, emita los mandatos siguientes:

     ```
     cd install_dir/itm/tables
     ../bin/itmcmd agent -o instance_name start sk
     ```

   - Desde la interfaz gráfica de usuario de CandleManage, seleccione cada agente de supervisión, pulse el botón derecho sobre él y seleccione **Iniciar**.

Resultados

Para revisar los resultados de rastreo, ubique los archivos de anotaciones en el directorio */dir_instalación*/itm/logs/.

El archivo de anotaciones que contiene la información de rastreo tiene el formato siguiente: `aaaapppptttt.log`, y el rastreo de la API tiene el formato siguiente: `aaaapppptttDsmQuery.out`, donde:

aaaa es el nombre de instancia del agente

pppp es el número de puerto del servidor

tttt es la indicación de fecha y hora

Por ejemplo:

`instancename15001111103143325000.log y hostname1500DsmQuery.out`

Rastreo del agente de Tivoli Monitoring para Tivoli Storage Manager en un sistema operativo Windows

Windows

Al utilizar Tivoli Monitoring para Tivoli Storage Manager, puede crear y configurar instancias de agentes que supervisen servidores de IBM Spectrum Protect. Para activar el rastreo de agentes de supervisión para servidores que se ejecuten en sistemas operativos Windows, detenga todas las instancias de agentes, modifique el archivo de configuración y reinicie las instancias de agentes.

Acerca de esta tarea

Antes de activar el rastreo, también puede abrir el espacio de trabajo de registro del agente Tivoli Enterprise Portal y el grupo de atributos del registro del agente y ver las actividades del agente. El espacio de trabajo de Anotaciones del agente contiene información acerca de cualquier servidor de IBM Spectrum Protect que tenga una instancia de agente configurada para supervisarlo.

Realice los pasos siguientes para activar el rastreo:

Procedimiento

1. Detenga las instancias del agente de supervisión completando los pasos siguientes:
   a. En el servidor de Tivoli Monitoring, pulse **Inicio** > **Todos los programas** > **IBM Tivoli Monitoring** > **Gestión de servicios de Tivoli Monitoring**.
   b. Seleccione cada instancia del agente de supervisión, pulse con el botón derecho y seleccione **Detener**.
2. Ubique el directorio donde se almacena el archivo de configuración:
   dir_instal\itm\tmaitm6

   Por ejemplo:
   C:\IBM\itm\tmaitm6
3. Para activar el rastreo de agente, asegúrese de que se ha establecido el valor siguiente en el archivo kskenv_*instanciaAgente*:
   KSK_TRACE=1
4. La interfaz de programación de aplicaciones (API) también se puede rastrear, pero no es necesaria a menos que lo solicite un representante de soporte de IBM. Para activar el rastreo para la API, asegúrese de que el siguiente valor se ha establecido en el archivo kskenv_*instanciaAgente*:
   KSK_APITRACE=1
5. Inicie las instancias del agente de Tivoli Monitoring para Tivoli Storage Manager completando los pasos siguientes:
   a. En el servidor de Tivoli Monitoring, pulse **Inicio** > **Todos los programas** > **IBM Tivoli Monitoring** > **Gestión de servicios de Tivoli Monitoring**.
   b. Seleccione cada agente de supervisión, pulse con el botón derecho y seleccione **Iniciar**.

Resultados

Los resultados de rastreo se ubican en el mismo directorio que el archivo de configuración:

dir_instal\itm\tmaitm6\logs

Los resultados del rastreo de la API se ubican en el siguiente directorio:
dir_instal\itm\tmaitm6

Por ejemplo:
```
C:\IBM\itm\tmaitm6\logs
C:\IBM\itm\tmaitm6
```

El archivo de anotaciones que contiene la información de rastreo tiene el formato `aaaapppptttt.log`, y el rastreo de la API tiene el formato `aaaapppptttDsmQuery.out`, donde:

aaaa es el nombre de instancia del agente

pppp es el número de puerto del servidor

tttt es la indicación de fecha y hora

Por ejemplo:
`instancename15001111103143325000.log y hostname1500DsmQuery.out`

Capítulo 8. Resolución de problemas de almacenamiento de datos

Si tiene un problema a la hora de almacenar o recuperar datos, estarán disponibles varios métodos para ayudarle a resolver el problema.

Resolución de problemas de datos ilegibles

Es posible que reciba datos ilegibles durante los procesos de importación o de replicación de nodo relacionados con una falta de conversión de la página de códigos durante estos procesos.

Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en las descripciones de dominios de políticas. Cualquier campo almacenado en el juego de caracteres de servidor y que utilice caracteres ASCII ampliados puede verse afectado.

Para resolver el problema, actualice los campos con los mandatos **UPDATE** adecuados después de la operación de importación o réplica de nodos.

Comprobar las anotaciones de actividades del servidor para resolver problemas de almacenamiento de datos

Compruebe si existen otros mensajes en las anotaciones de actividades del servidor correspondientes a los 30 minutos previos y a los 30 minutos posteriores al momento de producirse el error.

Emita el mandato **QUERY ACTLOG** para comprobar las anotaciones de actividades. Con frecuencia, el resto de los mensajes que se emiten pueden ofrecer información adicional acerca de la causa del problema y cómo resolverlo.

Comprobación de HELP para los mensajes emitidos para un problema de almacenamiento de datos

Comprobación en HELP de mensajes emitidos por IBM Spectrum Protect.

Los mensajes de IBM Spectrum Protect ofrecen información adicional en las secciones del mensaje **Explicación**, **Acción del sistema** o **Respuesta del usuario**. A menudo, esta información complementaria acerca del mensaje puede proporcionar los pasos necesarios para resolver el problema.

Reproducción del problema de almacenamiento de datos

Si un problema se puede reproducir con facilidad o de forma coherente, resulta posible identificar la causa del problema en una secuencia específica de eventos.

Los problemas de lectura o grabación de datos pueden estar relacionados con secuencias, en términos de las operaciones que se deben realizar, o pueden ser un error o una anomalía de un dispositivo subyacente.

Los problemas típicos relacionados con la secuencia de eventos se producen en volúmenes secuenciales. Un ejemplo sería que un volumen esté en uso para una copia de seguridad de cliente y que ese volumen se sustituya mediante una restauración de los datos de nodo de otro cliente. Esta sesión puede mostrarse como un error en la sesión de copia de seguridad del cliente que se ha sustituido. No obstante, esa sesión de copia de seguridad de cliente puede ser satisfactoria si se ha vuelto a intentar o si no se ha sustituido la primera vez.

Resolución de errores de almacenamiento de datos relacionados con la lectura o grabación en un dispositivo

Si el problema es un error que implica la lectura o escritura de datos de un dispositivo, muchos sistemas y dispositivos registran información en un archivo de anotaciones de errores del sistema. Por ejemplo, el archivo `errpt` para AIX y el archivo `Event Log` para Windows.

Si un dispositivo o volumen utilizado por informa de un error al archivo de registro de errores del sistema, se trata probablemente un problema de dispositivos. Los mensajes de error registrados en el archivo de registro de errores del sistema pueden proporcionar información suficiente para resolver el problema.

Cambio de la jerarquía de almacenamiento para resolver problemas de almacenamiento de datos

La jerarquía de almacenamiento incluye las agrupaciones de almacenamiento y las relaciones entre las agrupaciones de almacenamiento del servidor.

El agente de almacenamiento también utiliza las definiciones de agrupaciones de almacenamiento. Si se han cambiado los atributos de una agrupación de almacenamiento, puede afectar a las operaciones de almacenamiento y recuperación de datos. Revise los cambios en la jerarquía de almacenamiento y en las definiciones de agrupaciones de almacenamiento. Emita el mandato **QUERY ACTLOG** para ver el historial de mandatos o cambios que pueden afectar a las agrupaciones de almacenamiento. Además, utilice los mandatos **QUERY** siguientes para determinar si se han efectuado cambios:

- QUERY STGPOOL F=D

  Revise la configuración de la agrupación de almacenamiento. Si una agrupación de almacenamiento no está disponible, no se puede acceder a los datos de esa agrupación de almacenamiento. Si una agrupación de almacenamiento sólo es de lectura, los datos no se pueden grabar en esa agrupación. Si se da cualquier situación del caso, revise el motivo por el que estos valores se establecieron y considere la posibilidad de emitir el mandato **UPDATE STGPOOL** para establecer la agrupación en READWRITE. Otra consideración sería revisar el número de volúmenes reutilizables para una agrupación de almacenamiento de medios secuenciales.

- QUERY DEVCLASS F=D

  Las agrupaciones de almacenamiento pueden verse afectadas por los cambios en las clases de dispositivos. Revise la configuración de las clases de dispositivo para las agrupaciones de almacenamiento, incluidas la comprobación de las definiciones de biblioteca, unidad y vía de acceso. Emita los mandatos **QUERY LIBRARY**, **QUERY DRIVE** y **QUERY PATH** para agrupaciones de almacenamiento de medios secuenciales.

Cambio de las políticas de servidor para resolver problemas de almacenamiento de datos

Los atributos de políticas de servidor que están directamente relacionados con el almacenamiento de datos son los destinos de grupos de copias de los grupos de copia de seguridad y archivado. Del mismo modo, la clase de gestión, MIGDESTINATION, también afecta a la ubicación donde se almacenan los datos.

Revise los cambios en las políticas de almacenamiento del servidor. Emita el mandato **QUERY ACTLOG** para ver el historial de mandatos o cambios que pueden afectar a las políticas de almacenamiento. Además, utilice los mandatos **QUERY** siguientes para determinar si se han efectuado cambios:

- QUERY COPYGROUP F=D

  Revise la configuración de DESTINATION para los grupos de copias TYPE=BACKUP y TYPE=ARCHIVE. Revise también el "Destino migración" de las clases de gestión que utilizan los clientes HSM. Si los destinos de agrupación de almacenamiento se han cambiado y las operaciones de lectura o grabación de datos resultantes ahora fallan, evalúe los cambios efectuados y corrija el problema o vuelva a la configuración anterior.
- QUERY NODE F=D

  La asignación de un nodo a otro dominio puede afectar a las operaciones de lectura o grabación de datos de ese cliente. Concretamente, el nodo puede que se dirija a destinos de agrupación de almacenamiento que no sean los adecuados según los requisitos de ese nodo. Por ejemplo, podría asignarse a un dominio que no tenga ningún destino de grupo de copias TYPE=ARCHIVE. Si este nodo intenta archivar datos, fallará.

Resolución de un problema de copia de seguridad o de copia de almacenamiento de datos que únicamente se produce con un nodo específico

Si no puede realizar una copia de seguridad o copiar datos en un nodo específico, puede que no haya ninguna agrupación de datos activa en sus destinos activos. Estos están especificados en el dominio de políticas del nodo.

Emita el mandato `QUERY NODE` *`nombre_nodo`* `F=D` para verificar si el nodo que está almacenando los datos tiene autorización. El mandato **QUERY NODE** encuentra el nombre de dominio de políticas al que está asignado el nodo. Emita `QUERY DOMAIN` *`nombre_dominio`* donde *nombre_dominio* es la salida recuperada del mandato **QUERY NODE** anterior. Examine el parámetro **ACTIVEDESTINATION** para ver la lista de puertos de datos activos. Si la agrupación de datos activos en la que desea almacenar datos no está en la lista, emita el mandato **UPDATE DOMAIN** para añadir la agrupación de datos activos a la lista.

Resolución de un problema de almacenamiento de datos que únicamente se produce para un volumen específico

Si los problemas se dan sólo en un volumen de almacenamiento concreto, puede que el error sea del propio volumen, tanto si se trata de un volumen de medios secuenciales o DISK.

Si se trata de una operación de grabación de datos, emita el mandato `UPDATE VOLUME *volumeName* ACCESS=READONLY` para establecer este volumen en READONLY y vuelva a intentar la operación. Si la operación se realiza correctamente, intente establecer el volumen original en READWRITE emitiendo el mandato `UPDATE VOLUME *nombre_volumen* ACCESS=READWRITE`. Vuelva a intentar la operación. Si la operación falla únicamente cuando se utiliza este volumen, considere la posibilidad de emitir el mandato **AUDIT VOLUME** para evaluar este volumen y emita el mandato **MOVE DATA** para trasladar los datos de este volumen a otros volúmenes en la agrupación de almacenamiento. Una vez que se han trasladado los datos fuera de este volumen, suprima el volumen emitiendo el mandato **DELETE VOLUME**.

Consejos y sugerencias relativos al almacenamiento

Los consejos y las sugerencias que se recopilan aquí son de experiencias de problemas reales. Es posible que una de las soluciones sea la adecuada para su problema de IBM Spectrum Protect.

Consejos y sugerencias para el controlador de dispositivo

Puede que los problemas de los controladores de dispositivos se atribuyan con el sistema operativo, con la aplicación que utiliza el dispositivo, con el firmware de dispositivo o con el propio hardware de dispositivo.

Siempre que se detecte un problema relacionado con un dispositivo, pregúntese: "¿Ha cambiado algo?"

Si se ha cambiado el firmware del adaptador, puede que ello dé lugar a que un dispositivo experimente anomalías intermitentes o permanentes. Intente volver a establecer la versión anterior del firmware para determinar si el problema sigue produciéndose.

Si se ha cambiado el cableado existente entre el sistema y el dispositivo, este cambio, con frecuencia, contribuye a que se generen anomalías intermitentes o permanentes. Compruebe los cambios de cableado que se han realizado para verificar si son correctos.

Si se ha cambiado el firmware del dispositivo, puede que un dispositivo experimente anomalías intermitentes o permanentes. Intente volver a establecer la versión anterior del firmware para determinar si el problema sigue produciéndose.

Para conexiones SCSI, una patilla doblada en el cable SCSI donde se conecta con el sistema (o con el dispositivo) puede provocar errores para ese dispositivo o para cualquier dispositivo del mismo bus SCSI. Debe repararse o sustituirse cualquier cable con una patilla doblada. De forma parecida, deben terminarse los buses SCSI. Si se termina un bus SCSI de forma inadecuada, los dispositivos del bus pueden mostrar problemas intermitentes, o los datos transferidos por el bus pueden presentar daños. Compruebe los terminadores de bus SCSI para asegurarse de que son correctos.

Recuerde: Si la información de "consejos y sugerencias" no trata adecuadamente su problema con el controlador de dispositivo o si ésta es la configuración inicial de los controladores de dispositivos del sistema, compruebe que los dispositivos de hardware reciban soporte. Consulte el Portal de soporte.

Ajuste en los cambios del sistema operativo

El mantenimiento del sistema operativo puede cambiar los niveles de kernel, los controladores de dispositivo u otros atributos del sistema que pueden afectar a un dispositivo.

De forma similar, la actualización de la versión o del release del sistema operativo puede dar lugar a problemas de compatibilidad de dispositivos. Si es posible, vuelva a establecer el sistema operativo en el estado en el que se encontraba antes de que se produjera el error de dispositivo. Si no es posible llevar a cabo la reversión, compruebe si existen actualizaciones del controlador de dispositivo que podrían ser necesaria basándose en este nivel de arreglo, release o versión del sistema operativo.

Ajuste en los cambios en el adaptador SCSI o HBA en conexión con el dispositivo

Un controlador de dispositivo se comunica con un dispositivo determinado mediante un adaptador.

Si se trata de un dispositivo conectado mediante un canal de fibra, el controlador de dispositivo utiliza un adaptador de bus de host (HBA) para comunicarse. Si el dispositivo se conecta por SCSI, el controlador de dispositivo utiliza un adaptador SCSI para comunicarse. En cualquier caso, si el firmware del adaptador se ha actualizado o se ha sustituido el propio adaptador, el controlador de dispositivo puede experimentar problemas a la hora de utilizar el dispositivo.

Colabore con el proveedor del adaptador para verificar que se encuentra adecuadamente instalado y configurado. La siguiente lista muestra el resto de los posibles pasos:

- Si se ha cambiado el adaptador, intente volver a establecer el adaptador anterior para determinar si con ello se soluciona el problema.
- Si se ha cambiado otro hardware del sistema o si el sistema se ha abierto, vuelva a abrir el sistema y compruebe si el adaptador se ha instalado correctamente en el bus. Al abrir y cambiar otro hardware del sistema, puede que las tarjetas y otras conexiones del sistema hayan quedado incorrectamente instaladas, lo que podría provocar problemas intermitentes o una anomalía general de los dispositivos o de otros recursos del sistema.

Resolución de un problema de conexión con un cable suelto

Si está floja la conexión desde el dispositivo al cable o desde el cable al dispositivo, se pueden producir problemas en el dispositivo.

Compruebe las conexiones y verifique si las conexiones de los cables son correctas y si se han conectado firmemente.

Para los dispositivos SCSI, compruebe que los terminadores SCSI son correctos y que no existe ninguna patilla doblada en el propio terminador. Un bus SCSI terminado de forma inadecuada podría causar problemas de difícil solución relacionados con uno o varios dispositivos de ese bus.

Resolución de mensajes de error en las anotaciones de errores del sistema

Un dispositivo puede intentar notificar un error en las anotaciones de errores del sistema.

A continuación, se ofrecen algunos ejemplos de diversas anotaciones de errores del sistema:

- AIX `errpt`
- Windows `Registro de sucesos`

Los registros de errores del sistema pueden ser útiles porque los mensajes y la información que se anotan pueden ayudar a informar del problema o porque los mensajes podrían incluir recomendaciones relacionadas con la resolución del problema.

Consulte los registros de errores adecuados y realice todas las acciones basándose en los mensajes emitidos para el registro de errores.

Soporte de módulos de kernel de Linux de 32 bits o 64 bits para aplicaciones de 32 bits o 64 bits

Linux

Los módulos de kernel de Linux controlan el modo de bits del controlador de dispositivo de Linux SCSI genérico, de todos los controladores de HBA (Host Bus Adapter) y otros valores.

Todos estos módulos de kernel sólo soportan aplicaciones que poseen el mismo modo de bits con los módulos de kernel en ejecución. En otras palabras, los módulos de kernel de 64 bits sólo admiten aplicaciones de 64 bits en los sistemas Linux de 64 bits.

Si una aplicación de 32 bits se ejecuta en Linux de 64 bits, el sistema invoca un módulo de kernel de 64 bits; la aplicación de 32 bits provoca un error de segmentación en el. También se produce un error de segmentación si una aplicación de 64 bits invoca un módulo de kernel de 32 bits en un sistema Linux de 32 bits.

Para evitar estos errores de segmentación, asegúrese de que el modo de bits del módulo de kernel de Linux y de sus aplicaciones sean los mismos verificando que las aplicaciones de 32 bits solo puedan invocar módulos de kernel de 32 bits en sistemas Linux de 32 bits y que las aplicaciones de 64 bits solo puedan invocar módulos de kernel de 64 bits en sistemas Linux de 64 bits.

Ejecución de un servidor IBM Spectrum Protect de Linux en una arquitectura x86_64

Linux

Los sistemas operativos Linux de 32 y 64 bits pueden ejecutarse en sistemas AMD64 y EM64T, los cuales son sistemas de 64 bits.

Un agente de almacenamiento y un servidor de IBM Spectrum Protect en Linux de 64 bits sólo pueden ejecutarse en un sistema AMD64/EM64T con un sistema operativo Linux de 64 bits. De igual modo, un agente de almacenamiento y un servidor IBM Spectrum Protect Linux de 32 bits sólo pueden ejecutarse en un sistema AMD64/EM64T con un sistema operativo Linux de 32 bits.

Un servidor IBM Spectrum Protect de 64 bits que emita el mandato **QUERY SAN** precisa una API HBA (Host Bus Adapter) de 64 bits en un sistema AMD64/EM64T. Si un sistema AMD64 está equipado con un HBA Qlogic, podría crear un problema debido a que, de forma predeterminada, Qlogic proporciona una API HBA de 32 bits en el sistema AMD64. Debe instalar una API HBA de 64 bits en el sistema antes de emitir el mandato **QUERY SAN** de 64 bits.

Ajuste de los cambios en el controlador HBA en los kernels de Linux 2.6.x

El cambio más claro para los controladores HBA en los kernel de Linux 2.6.x es que todos los controladores tienen "ko" como nuevo sufijo.

A continuación, se indican los nombres y las ubicaciones de los controladores en los kernels 2.6.x:

Adaptec
El controlador (`aic7xxx.ko`) se encuentra en el directorio `/lib/modules/kernel-level/drivers/scsi/aic7xxx/`.

Emulex
El controlador (`lpfcdd.ko`) se encuentra en el directorio `/lib/modules/kernel-level/drivers/scsi/lpfc/`.

Qlogic
Sus nombres de controlador son `qla2xxx.ko`, `qla2100.ko`, `qla2200.ko`, `qla2300.ko`, `qla2322.ko`, etc. Existe un orden concreto para cargar los controladores HBA. `qla2xxx.ko` es un controlador básico y se debe cargar en primer lugar. Después de cargar el controlador `qla2xxx.ko`, el sistema debe cargar entonces el controlador `qla2300.ko` si está equipado con una tarjeta Qla2300. Todos los controladores se encuentran en el directorio `/lib/modules/kernel-level/drivers/scsi/qla2xxx/`.

Habilitar la compatibilidad con varios LUN en kernels Linux

Linux

Para configurar los dispositivos SCSI con varios LUN en un sistema Linux, el kernel de Linux debe configurarse para habilitar la admisión de varios LUN.

Sin embargo, la admisión de varios LUN en algunas distribuciones de Linux no es una opción predeterminada y precisa que los usuarios agreguen manualmente esta opción al kernel en ejecución. Siga estos pasos para activar varios LUN en arquitectura IA32:

1. Agregue un parámetro a un archivo de configuración del cargador.
   - Para un cargador LILO:
     a. Añada append="max_scsi_luns=128" al archivo `/ect/lilo.conf`.
     b. Ejecute el lilo.
   - Par aun cargador GRUB:
     a. Agregue max_scsi_luns=128 después de la lista de imágenes del kernel en el archivo `/etc/grub.conf` para la distribución de RedHat.
     b. Agregue max_scsi_luns=128 después de la lista de imágenes del kernel en el archivo `/boot/grub/menu.1` para la distribución de SuSE.
2. Reinicie el sistema.

Utilización de IBM Spectrum Protect para ejecutar un ddtrace en Linux

Linux

El controlador de dispositivo passthru se puede rastrear emitiendo el mandato **DDTRACE**.

Para activar el rastreo, emita los siguientes comandos desde la consola de servidor o el cliente de administración:

```
trace
enable lpdd <otros nombres de clases de rastreo de servidor>
trace begin <nombre archivo>
```

Seleccione una de las siguientes tres opciones:

- ddtrace start librarydd tapedd (para rastrear tanto la biblioteca como la unidad)
- ddtrace start librarydd (rastreo sólo de la biblioteca)
- ddtrace start tapedd (rastreo sólo de la unidad)

Recuerde: No se precisan **DDTRACE GET** ni **DDTRACE END**.

No se puede activar el rastreo del controlador del dispositivo de paso a través de IBM Spectrum Protect mediante la herramienta ddtrace.

Actualización de la información de dispositivos de sistemas host en una red SAN dinámica sin reiniciarla

Cuando cambian los dispositivos en un entorno SAN, la información sobre este entorno modificado no se envía automáticamente a los hosts conectados a la SAN.

Si la información de dispositivo no se ha actualizado en los hosts conectados a la SAN, las vías de acceso de dispositivo definidas previamente ya no existen. Si utiliza la información de dispositivo existente para definir vías de acceso de dispositivo, copias de seguridad o datos de restauración, esas operaciones pueden resultar fallidas. Para evitar ese tipo de errores, utilice un método distinto para cada sistema operativo a fin de actualizar la información de dispositivo en la SAN sin reiniciar los sistemas host.

AIX Emita el mandato **CFGMGR** para forzar una reconfiguración del sistema operativo por su cuenta. A continuación, ejecute SMIT para volver a configurar los dispositivos de IBM Spectrum Protect.

Linux No hay un mandato del sistema para volver a configurar el sistema operativo. Para volver a explorar los canales de fibra y los buses SCSI, los controladores de adaptador correspondientes a estos adaptadores de canal de fibra y adaptadores SCSI se deben descargar y volver a cargar de nuevo en el kernel de Linux. Después de volver a cargar los controladores HBA, ejecute **autoconf** o **TSMSCSI** para volver a configurar los dispositivos de IBM Spectrum Protect en Linux. Puede emitir el mandato **LSPCI** para descubrir qué adaptadores SCSI y de canal de fibra están disponibles en el sistema. El mandato **RMMOD** descarga un controlador del kernel y el mandato **MODPROBE** carga un controlador en el kernel.

Tabla 14. Adaptadores HBA y los controladores correspondientes para todas las arquitecturas de Linux

Adaptadores HBA	Nombre de controlador HBA	Arquitecturas disponibles
Adaptec 7892	aix7xxx	IA32, AMD64

Tabla 14. Adaptadores HBA y los controladores correspondientes para todas las arquitecturas de Linux (continuación)

Adaptadores HBA	Nombre de controlador HBA	Arquitecturas disponibles
Qlogic 22xx	qla2200	IA32, AMD64
Qlogic 23xx	qla2300	IA32, AMD64
Qlogic 2362	qla2362	EM64T
Emulex	lpfcdd	IA32, iSeries, pSeries

Establecimiento de las opciones de varios LUN como "activadas" para la configuración de Adaptec SCSI y Qlogic Fibre-Channel HBA BIOS en Linux

De forma predeterminada, los adaptadores de Adaptec SCSI "desactivan" la opción de varios LUN (número de unidad lógica) en sus BIOS, lo que hace que el controlador de adaptador SCSI no pueda analizar una unidad SCSI con varios LUN de forma adecuada.

Procedimiento

La opción de varios LUN debe estar activada. Siga los pasos siguientes para activar varias opciones de LUN:

1. Pulse las teclas Control y A al mismo tiempo.
2. Seleccione **SCSI Device Configuration** en el valor **Configure/View Host Adapter**.
3. Cambie No por Yes en Bios Multiple LUN support.

Activación de la opción de habilitación de cinta:

De forma predeterminada, los adaptadores de bus de host de Qlogic Fibre establecen la opción de habilitación de cinta como desactivada en la BIOS, lo cual afecta a la ejecución de algunos mandatos SCSI en varios dispositivos de cinta SCSI.

Procedimiento

La opción de habilitación de cintas debe estar activada. Siga los pasos siguientes para activar las opción de activación de cinta.

1. Pulse las teclas Alt y Q al mismo tiempo.
2. Seleccione **Advanced Settings**.
3. Cambie Disable por Enable en Fibre Channel Tape Support.

Consejos y sugerencias para los subsistemas de disco y unidades de disco duro

El servidor de IBM Spectrum Protect necesita que las unidades de disco duro, los subsistemas de disco, los sistemas de archivos de terceros y los sistemas de archivos remotos se comporten de una determinada manera. Este comportamiento específico permite que IBM Spectrum Protect administre y almacene los datos adecuadamente asegurando la integridad del propio servidor.

Las definiciones siguientes se ofrecen para ayudarle a comprender mejor las unidades de disco duro y los subsistemas de disco:

Unidad de disco duro

Un dispositivo de almacenamiento de unidad de disco duro se instala habitualmente en un sistema específico y se utiliza para el almacenamiento por parte de un servidor de IBM Spectrum Protect en ese sistema.

Subsistema de disco

Es un subsistema de disco externo que se conecta con un sistema por medio de una SAN (storage area network) o de otro mecanismo. Por lo general, los subsistemas de disco se encuentran fuera del sistema con el que se conectan y pueden ubicarse muy cerca de éste o muy lejos. Puede que estos subsistemas dispongan de algún método para colocar en la memoria caché las peticiones de entrada/salida para los discos. Si los datos se encuentran en la memoria caché, pese a la existencia de una solicitud de omisión de la memoria caché que se puede producir en sistemas de archivos remotos y determinados subsistemas de disco, se pueden producir anomalías de entrada/salida. Las anomalías se deben a una diferencia entre el rastreo de IBM Spectrum Protect y los datos realmente residentes en un sistema de archivos. Los sistemas de archivos remoto y los subsistemas de disco que muestren estas características no están admitidos. Con frecuencia, los subsistemas de disco disponen de su propio software de configuración y gestión. Un subsistema de disco debe notificar los resultados de forma sincrónica.

El servidor puede definir unidades de disco duro y subsistemas de disco que utiliza el sistema o el sistema operativo en el sistema donde está instalado IBM Spectrum Protect. Normalmente, se define una unidad de disco duro o un subsistema de disco en el sistema donde se ha instalado IBM Spectrum Protect como una unidad o sistema de archivos. Después de definir en el sistema operativo la unidad de disco duro o el subsistema de disco, IBM Spectrum Protect puede utilizar este espacio mediante la asignación de una base de datos, anotación de recuperación o volumen de agrupación de almacenamiento en el dispositivo. Posteriormente, el volumen de IBM Spectrum Protect tendrá el mismo aspecto que otro archivo de esa unidad o sistema de archivos.

Omisión de la memoria caché durante las operaciones de grabación

La base de datos, los registros de recuperación y los volúmenes de agrupaciones de almacenamiento se abren con la configuración adecuada del sistema operativo para solicitar que las peticiones de grabación de información omitan cualquier caché y se graben directamente en el dispositivo.

Al omitir la caché durante las operaciones de grabación, IBM Spectrum Protect mantiene la integridad de la información y los atributos de los clientes. Es necesario omitir la caché. Si un evento externo, como una interrupción del suministro eléctrico, provoca que el servidor o el sistema donde el servidor está instalado se detenga o deje de funcionar mientras el servidor está funcionando, los datos de la memoria caché puede que se graben o no en el disco. Si los datos de IBM Spectrum Protect en la caché de disco no se graban satisfactoriamente en el disco, la información de la base de datos del servidor o las anotaciones de recuperación puede que no estén completas. Igualmente, es posible que no se encuentre la información que se debía guardar en los volúmenes de agrupación de almacenamiento.

La omisión de la memoria caché no es realmente un problema para las unidades de disco duro instaladas en el sistema donde el servidor está instalado y en ejecución. En este caso, la configuración del sistema operativo que se utiliza cuando IBM Spectrum Protect abre los volúmenes en esa unidad de disco duro

administran generalmente el comportamiento de la caché de forma adecuada y aplican la solicitud para impedir el almacenamiento en la caché de operaciones de grabación.

Por lo general, el uso y la configuración de la memoria caché para subsistemas de disco supone un problema mayor, debido a que los subsistemas de disco, con frecuencia, no reciben información del sistema operativo relacionada con la no utilización de la memoria caché para las operaciones de grabación. Los subsistemas de disco también pueden ignorar esta información cuando se abra un volumen. Por lo tanto, el almacenamiento en la caché de operaciones de grabación puede provocar daños en la base de datos del servidor o la pérdida de información del cliente o ambas situaciones. Los problemas dependen de qué volúmenes de IBM Spectrum Protect se definan en el subsistema de disco y de la cantidad de pérdida de datos en la memoria caché. Los subsistemas de disco deben configurarse para que no almacenen en la caché operaciones de grabación cuando se definen en este disco una anotación de recuperación, un volumen de agrupación de almacenamiento o una base de datos de IBM Spectrum Protect. Otra alternativa es utilizar la caché no volátil para el subsistema de disco. La caché no volátil utiliza una batería de reserva u otro tipo de esquema para que el contenido de la caché pueda grabarse en el disco en caso de que se produzca una anomalía.

Traslado de los datos existentes a otros volúmenes antes de modificar o mover la base de datos

El tamaño y la ubicación de los volúmenes (archivos) de agrupación de almacenamiento de IBM Spectrum Protect no pueden cambiar después de haber sido definidos y utilizados por el servidor.

Si el tamaño cambia o el archivo se mueve, la información interna que IBM Spectrum Protect utiliza para describir el volumen puede que ya no coincida con los atributos reales del archivo. Si necesita mover o cambiar el tamaño de un volumen de agrupación de almacenamiento de IBM Spectrum Protect, mueva la información a otros volúmenes antes de modificar o mover la base de datos.

Asignación del directorio FILE entre agentes de almacenamiento y servidores para archivos compartidos

Los agentes de almacenamiento y los servidores de IBM Spectrum Protect pueden acceder a los mismos datos de las clases de dispositivos FILE si se define un conjunto de directorios que deben utilizarse en una definición de clase de dispositivos.

El nombre de directorio en una definición de clase de dispositivo FILE identifica la ubicación donde el servidor coloca los archivos que representan volúmenes de almacenamiento para esta clase de dispositivo. Cuando ejecuta el mandato **DEFINE DEVCLASS**, el servidor amplía el nombre de directorio especificado en su formatos totalmente calificado, comenzando por el directorio raíz.

Puede especificar uno o más directorios como ubicación de los archivos utilizados en la clase de dispositivo FILE. La ubicación predeterminada es el directorio de trabajo actual del servidor en el momento en el que se emite el mandato. Puede especificar los directorios para AIX o Linux.

No especifique varios directorios en el mismo sistema de archivos ya que pueden producirse cálculos de espacio incorrectos. Por ejemplo, si los directorios `/usr/dir1` and `/usr/dir2` están en el mismo sistema de archivos, la comprobación de espacio contará cada directorio como un sistema de archivos independiente. La comprobación de espacio realiza una evaluación preliminar del espacio disponible

durante operaciones de almacenamiento. Si los cálculos de espacio son incorrectos, el servidor podría asignar una agrupación de almacenamiento FILE pero no podría obtener espacio, lo que provocaría que el funcionamiento fuera anómalo. Si la comprobación de espacio es precisa, el servidor puede pasar por alto la agrupación FILE en la jerarquía de almacenamiento y utilizar la siguiente agrupación de almacenamiento, si hay alguna disponible.

Si el servidor necesita asignar un volumen reutilizable, creará un nuevo archivo en el directorio o directorios especificados. (El servidor puede elegir cualquiera de los directorios para crear nuevos volúmenes reutilizables). Con el fin de optimizar el rendimiento, asegúrese de los distintos directorios correspondan a distintos volúmenes físicos.

Consulte la tabla siguiente para conocer la extensión de nombre de archivo creada por el servidor para los volúmenes reutilizables en función del tipo de datos que se almacenan.

Tabla 15. Extensiones de nombre de archivo para volúmenes reutilizables

Para los volúmenes reutilizables usados para almacenar los datos de:	**La extensión de archivo es:**
Clientes	`.BFS`
Exportación	`.EXP`
Copia de seguridad de la base de datos	`.DBV`

Por cada agente de almacenamiento que comparte el acceso a **FILE**, las **PATH** definidas para cada **DRIVE** vista por el agente de almacenamiento deben ofrecer acceso al mismo conjunto de directorios. Cuando las **PATH** se definen, los directorios de cada agente de almacenamiento deben coincidir en número y orden respecto a los directorios, tal como aparece en la definición de clase de dispositivos en el servidor. Si estas definiciones no están sincronizadas, puede que el agente de almacenamiento no sea capaz de acceder a los volúmenes FILE, lo que producirá restauraciones de la LAN correctas y anomalías de montaje en las operaciones de restauración fuera de la LAN.

Consejos y sugerencias de las unidades de cinta y de las bibliotecas

Los problemas con unidades de cinta y bibliotecas podrían estar relacionados con el software del sistema que intenta utilizar el dispositivo, las conexiones con el dispositivo o el dispositivo.

Siempre que se detecte un problema relacionado con un dispositivo, pregúntese: "¿Ha cambiado algo?" Posiblemente el origen del problema se hallará entre el sistema que intenta utilizar el dispositivo. O tenga en cuenta el propio dispositivo, en especial si el dispositivo funcionaba correctamente antes de la realización de un cambio determinado y, tras haberlo realizado, el dispositivo ha dejado de funcionar.

- Si se ha cambiado el firmware del adaptador, puede que un dispositivo experimente anomalías intermitentes o permanentes. Intente volver a establecer la versión anterior del firmware para determinar si el problema sigue produciéndose.
- Si se ha cambiado el cableado existente entre el sistema y el dispositivo, se pueden producir fallos intermitentes o persistentes. Compruebe los cambios de cableado que se han realizado para verificar si son correctos.

- Si se ha cambiado el firmware del dispositivo, puede que un dispositivo experimente anomalías intermitentes o permanentes. Intente volver a establecer la versión anterior del firmware para determinar si el problema sigue produciéndose.

Ajuste en los cambios del sistema operativo

El mantenimiento del sistema operativo puede cambiar los niveles de kernel, los controladores de dispositivo u otros atributos del sistema que pueden afectar a un dispositivo. De forma similar, la actualización de la versión o del release del sistema operativo puede dar lugar a problemas de compatibilidad de dispositivos.

Si es posible, vuelva a establecer el sistema operativo en el estado en el que se encontraba antes de que se produjera la anomalía. Si no puede llevar a cabo la reversión del sistema operativo, compruebe si existen actualizaciones del controlador de dispositivo que podrían ser necesaria basándose en el nivel de arreglo, release o versión del sistema operativo.

Cómo adaptarse a los cambios del controlador de dispositivo

Una actualización de un controlador de dispositivo puede dar como resultado que el dispositivo de unidad de cinta o de biblioteca deje de funcionar. Estos problemas también pueden producirse a consecuencia del tipo de controlador que se utiliza.

Cuando trabaja con las bibliotecas o las unidades de IBM, a diferencia de utilizar bibliotecas y unidades de otros proveedores, el tipo de controlador de dispositivo que elija resulta importante. Las bibliotecas y unidades de IBM deben utilizar el controlador de dispositivo de IBM, mientras que las bibliotecas y unidades de otros proveedores deben utilizar el controlador de dispositivo de IBM Spectrum Protect.

Vuelva a establecer la versión anterior del controlador de dispositivo para determinar si el problema se debe a la versión más reciente del controlador.

Cómo adaptarse a un adaptador sustituido y otro cambio de hardware

Una conexión pequeña con la interfaz del sistema (SCSI) al dispositivo utiliza un adaptador SCSI. Una conexión de canal de fibra (óptica) con el dispositivo utiliza un adaptador de bus de host (HBA).

En cualquiera de los dos casos, la causa del problema podría ser desde un adaptador cambiado o un sistema abierto donde se ha cambiado o arreglado otro hardware.

Recuerde: Al punto de conexión para conectar el dispositivo con el sistema se le conoce como adaptador. Otro término para adaptador es *tarjeta*.

Consulte la siguiente información que puede servirle de ayuda para realizar ajustes respecto a un adaptador o hardware reemplazado.

- Si se ha cambiado el adaptador, vuelva al adaptador anterior para determinar si con ello se soluciona el problema.
- Si se ha cambiado hardware del sistema o si el sistema se ha abierto, compruebe el sistema para asegurarse de que el adaptador se ha instalado correctamente en el bus. Al abrir y cambiar otro hardware del sistema, puede que las tarjetas y otras conexiones del sistema hayan quedado incorrectamente instaladas. La instalación incorrecta de las conexiones puede provocar problemas intermitentes o una anomalía general de los dispositivos o de otros recursos del sistema.

Resolución de un problema de conexión con un cable suelto

Puede que se produzcan problemas relacionados con el dispositivo si existe una conexión suelta entre el sistema y el cable o entre el cable y el sistema.

Compruebe las conexiones y verifique si las conexiones de los cables son correctas y si se han conectado firmemente.

Para los dispositivos SCSI, compruebe que los terminadores SCSI son correctos y que no existe ninguna patilla doblada en el propio terminador. Un bus SCSI terminado de forma inadecuada podría causar problemas con uno o varios dispositivos de ese bus.

Utilización de mensajes de error para resolver un problema de funcionamiento erróneo de un dispositivo

Puede que un dispositivo intente informar de un error en las anotaciones de errores del sistema, donde podrá encontrar la causa del problema.

A continuación se muestran diversas anotaciones de errores del sistema:

- `errpt` para AIX
- `Registro de eventos` para Windows

Las anotaciones de errores del sistema pueden ser útiles, porque los mensajes y la información que se anotan pueden ayudar a informar del problema o porque los mensajes podrían incluir recomendaciones relacionadas con la resolución del problema. Consulte las anotaciones de errores adecuadas y realice las acciones recomendadas basándose en los mensajes emitidos para las anotaciones de errores.

Consejos y sugerencias de SAN

Los problemas con una SAN (red de área de almacenamiento) podrían estar relacionados con el software del sistema que intenta utilizar el dispositivo, las conexiones con el dispositivo o el dispositivo.

Siempre que se detecte un problema relacionado con una SAN, pregúntese: "¿Ha cambiado algo?" Cualquier tipo de cambio realizado puede ser sospechoso, desde el sistema que utiliza el dispositivo hasta el propio dispositivo, especialmente si el dispositivo funcionaba antes de producirse el cambio y se detuvo después de que se produjera.

Para entender mejor cómo diagnosticar los problemas con un SAN, revise la terminología siguiente y las abreviaturas normales:

Canal de fibra
: El canal de fibra indica que existe una conexión de fibra óptica con un dispositivo o componente.

Adaptador de bus de host
: Un adaptador de bus de host (HBA) permite a un sistema dado acceder a un SAN. En cuanto a sus funciones, un HBA es similar a un adaptador de red en que éste proporciona a un sistema acceso a una LAN (red de área local) o a una WAN (red de área amplia).

SAN
: Un SAN es una red de dispositivos compartidos a la que se accede normalmente mediante fibra. Con frecuencia, un SAN se utiliza para compartir dispositivos entre muchos sistemas distintos.

Comprenda su configuración de SAN

Comprender la configuración de SAN es vital en los entornos SAN. Diversas implementaciones de la SAN tienen limitaciones o requisitos relacionados con la configuración e instalación de los dispositivos.

Las tres configuraciones de SAN son punto a punto, bucle arbitrado y tejido conmutado.

Punto a punto
Los dispositivos se conectan directamente con el adaptador de bus de host (HBA).

Bucle arbitrado
Las topologías de bucle arbitrado son topologías en anillo y su limitación es el número de dispositivos que se admiten en el bucle y el número de dispositivos que pueden utilizarse en un momento determinado. En un bucle arbitrado, sólo pueden comunicarse simultáneamente dos dispositivos. Los datos que se leen desde un dispositivo o que se graban en un dispositivo se transfieren desde un dispositivo del bucle hasta otro, hasta que llegan al dispositivo de destino. El principal factor limitador de un bucle arbitrado es que sólo pueden utilizarse dos dispositivos simultáneamente.

Tejido conmutado
En una SAN de tejido conmutado, todos los dispositivos del tejido serán dispositivos nativos de fibra. Esta es la topología que dispone de mayor ancho de banda y que ofrece más flexibilidad, pues todos los dispositivos están disponibles para todos los HBA por medio de alguna vía de acceso de fibra.

Asegúrese de que el HBA funciona con la red SAN

El adaptador de bus de host (HBA) es un dispositivo importante para el funcionamiento adecuado de un SAN. Los problemas que podrían producirse en relación con los HBA abarcan desde una configuración incorrecta hasta la existencia de un BIOS o de controladores de dispositivo no actualizados.

Para un HBA determinado, compruebe los siguientes elementos:

BIOS Los HBA incorporan un BIOS que puede actualizarse. El proveedor del HBA dispone de herramientas para actualizar el BIOS del HBA. Periódicamente deberán comprobarse los HBA de la SAN para determinar si existen actualizaciones de BIOS que deben aplicarse.

Controlador de dispositivo
Los HBA utilizan controladores de dispositivo para, en colaboración con el sistema operativo, proporcionar conectividad a la SAN. Por lo general, el proveedor facilitará un controlador de dispositivo para utilizarlo con el HBA del proveedor. Asimismo, el proveedor proporciona instrucciones y las herramientas necesarias para actualizar el controlador de dispositivo. Periódicamente deberá comprobarse el nivel del controlador de dispositivo con la información que proporciona el proveedor y, si es necesario, éste deberá actualizarse para que disponga de los últimos arreglos y soporte.

Configuración
Los HBA disponen de varios valores que pueden configurarse. Los valores suelen afectar al modo en que IBM Spectrum Protect funciona con un dispositivo SAN.

Referencia relacionada:

"Problemas de configuración de un HBA"

Problemas de configuración de un HBA

Los adaptadores de bus de host (HBA) disponen de muchos valores y opciones de configuración distintos.

Habitualmente el proveedor del HBA proporciona información acerca de la configuración del HBA y de los valores adecuados para esa configuración. Asimismo, el proveedor del HBA puede proporcionar un programa de utilidad y otras instrucciones relacionadas con la configuración del HBA. Los siguientes ajustes afectan al uso de IBM Spectrum Protect con una SAN:

- Topología de la red de área de almacenamiento (SAN)

  El HBA debe establecerse correctamente en función de la topología de la SAN que actualmente se utiliza. Por ejemplo, si la SAN es un bucle arbitrado, el HBA debe establecerse para esta configuración. Si el HBA se conecta con un conmutador, el puerto de este HBA debe establecerse como "punto a punto" y no como "bucle".

  Con la correlación de dispositivos de IBM Spectrum Protect SAN, puede completar el descubrimiento de SAN en la mayoría de los sistemas y el enlace permanente de los dispositivos no es necesario. Un servidor de IBM Spectrum Protect puede encontrar el dispositivo si la vía de acceso al dispositivo ha cambiado debido a un reinicio u otro motivo.

  Vaya al Portal de soporte para verificar el soporte a la plataforma, el proveedor de HBA o el nivel de controlador para el descubrimiento de SAN de IBM Spectrum Protect.
- Velocidad del enlace de canal de fibra.

  En la mayoría de las topologías de la SAN, la SAN se configura con una velocidad máxima. Por ejemplo, si la velocidad máxima del conmutador de canal de fibra es de 1 GB/s, el HBA debe también establecerse en este mismo valor. O bien el HBA debe establecer para la negociación automática (AUTO), si el HBA admite esta posibilidad.
- ¿Está activado el soporte de cintas de canal de fibra?

  IBM Spectrum Protect requiere que un HBA está configurado con soporte de cinta. IBM Spectrum Protect normalmente utiliza las redes SAN para acceder a unidades y bibliotecas de cinta. Por lo tanto, debe activarse el valor del HBA que admite cintas.

AIX Linux Para ayudar con la determinación de los problemas, puede utilizar el módulo `dsmsanlist` para obtener información sobre los dispositivos en una red de área de almacenamiento (SAN). El módulo `dsmsanlist` está instalado de forma predeterminada cuando el servidor de IBM Spectrum Protect o el agente de almacenamiento de IBM Spectrum Protect está instalado.

Problemas de configuración del conmutador de canal de fibra

Un conmutador de canal de fibra admite muchas configuraciones distintas. Los puertos del conmutador deben configurarse de acuerdo con el tipo de SAN que está configurado y para los atributos de la SAN.

El proveedor del conmutador, por lo general, proporciona información acerca de los valores y de la configuración adecuados en función de la topología de la SAN que se desea desplegar. Asimismo, el proveedor del conmutador debe proporcionar un programa de utilidad y otras instrucciones relacionadas con la configuración de éste. Los siguientes valores suelen afectar al modo en que IBM Spectrum Protect utiliza una red SAN conmutada:

Velocidad del enlace de canal de fibra
En la mayoría de las topologías de la SAN, la SAN se configura con una velocidad máxima. Por ejemplo, si la velocidad máxima del conmutador de canal de fibra es de 1 GB/s, el HBA debe también establecerse en este mismo valor. O bien el HBA debe establecer para la negociación automática (AUTO), si el HBA admite esta posibilidad.

Modalidad de puerto
Los puertos del conmutador deben configurarse correctamente para el tipo de topología de la SAN que se desea implementar. Por ejemplo, si la SAN es un bucle arbitrado, el puerto debe establecerse en PUERTO_FL. Otro ejemplo; si el HBA se conecta con un conmutador, las opciones del HBA deben establecerse en "punto a punto", no en "bucle."

Configuración del puerto de pasarela de datos

Una pasarela de datos en un SAN convierte el canal de fibra a SCSI para dispositivos SCSI conectados a la pasarela.

Las pasarelas de datos se utilizan muy comúnmente en las SAN, pues permiten utilizar dispositivos SCSI y, por lo tanto, es importante que los valores del puerto de una pasarela de datos sean correctos.

El proveedor de la pasarela de datos, por lo general, proporciona información acerca de los valores y de la configuración adecuados en función de la topología de la SAN que se desea desplegar y de los dispositivos SCSI que se desean utilizar. Asimismo, puede que el proveedor proporcione una herramienta y otras instrucciones relacionadas con la configuración de ésta. A continuación, se indican los valores que pueden utilizarse en la modalidad de puerto de canal de fibra del puerto conectado en una pasarela de datos:

Destino privado
Desde este puerto sólo pueden verse y utilizarse los dispositivos SCSI conectados con la pasarela de datos. Respecto a los dispositivos SCSI disponibles, la pasarela simplemente transfiere las tramas a un dispositivo de destino determinado. Los valores del puerto de destino privado generalmente se utilizan para los bucles arbitrados.

Destino privado e iniciador
Desde este puerto sólo pueden verse y utilizarse los dispositivos SCSI conectados con la pasarela de datos. Respecto a los dispositivos SCSI disponibles, la pasarela simplemente transfiere las tramas a un dispositivo de destino determinado. Como iniciador, esta pasarela de datos también podría iniciar y gestionar operaciones de traspaso de datos. De manera específica, existen comandos SCSI ampliados que admiten el traspaso de datos de terceros. Cuando un puerto determinado se establece como iniciador, éste puede seleccionarse para utilizarse para las peticiones SCSI de traspaso de datos de terceros.

Destino público
Desde este puerto pueden verse y utilizarse todos los dispositivos SCSI conectados con la pasarela de datos, así como otros dispositivos que estén disponibles desde el tejido.

Destino público e iniciador
Desde este puerto pueden verse y utilizarse todos los dispositivos SCSI conectados con la pasarela de datos, así como otros dispositivos que estén disponibles desde el tejido. Como iniciador, esta pasarela de datos también podría iniciar y gestionar operaciones de traspaso de datos. De manera específica, existen comandos SCSI ampliados que admiten el traspaso de

datos de terceros. Cuando un puerto determinado se establece como iniciador, éste puede seleccionarse para utilizarse para las peticiones SCSI de traspaso de datos de terceros.

Configuración de la red SAN entre dispositivos

Los dispositivos de una SAN, como una pasarela de datos o un conmutador, habitualmente proporcionan herramientas que muestran qué ve ese dispositivo en la SAN.

Estas herramientas pueden utilizarse para entender mejor la configuración de la SAN y para llevar a cabo la resolución de los problemas de la SAN. El proveedor de la pasarela de datos o del conmutador proporciona un programa de utilidad para la configuración. Como parte de este programa de utilidad de configuración hay información útil como:

- Cómo está configurado el dispositivo
- Otra información que el dispositivo ve en la topología SAN (de la que forma parte)

Utilice estos programas de utilidad del proveedor para verificar la configuración de la SAN entre dispositivos:

Pasarela de datos
La pasarela de datos informa de todos los dispositivos de canal de fibra y los dispositivos SCSI que están disponibles en la SAN.

Conmutador
Un conmutador proporciona información acerca del tejido de la SAN.

Informe de errores del enlace de canal de fibra

La mayoría de los dispositivos SAN proporcionan herramientas de supervisión que se pueden utilizar para notificar información sobre errores y estadísticas sobre rendimiento.

El proveedor del dispositivo debe proporcionar un programa de utilidad para la supervisión. Si se dispone de una herramienta de supervisión, ésta generalmente informará acerca de los errores. Se experimentan con más frecuencia los siguientes errores:

Error de CRC, código de error 8b/10b y otros síntomas similares
Estos errores pueden recuperarse y en los que el manejo de errores generalmente se proporciona mediante firmware o hardware. En la mayoría de los casos, el método de recuperación del dispositivo consiste en volver a transmitir la trama anómala. El enlace de canal de fibra sigue estando activo cuando se detectan estos errores. Las aplicaciones que utilizan un dispositivo de SAN y que experimentan este tipo de error de enlace por lo general no detectan el error, a menos que se trate de un error permanente. Un error permanente es un error en el que la recuperación del firmware y del hardware no puede volver a transmitir correctamente los datos después de haber realizado varios intentos. La recuperación para estos tipos de errores es, generalmente, muy rápida y no afectará al rendimiento del sistema.

Error de enlace (pérdida de señal, pérdida de sincronización, recepción de primitiva NOS)
Este error indica que existe un enlace que realmente se ha "interrumpido" durante un período de tiempo determinado. Probablemente se debe a un error en el conector de interfaz de gigabit (GBIC), en el adaptador de interfaz de medios (MIA) o en el cable. La recuperación para este tipo de

error conllevará una interrupción. Este error aparece en la aplicación que utiliza el dispositivo de SAN que ha experimentado este error de enlace. La recuperación deberá aplicarse en el nivel de intercambio de mandatos e implicará que la aplicación y el controlador de dispositivo deberán realizar un restablecimiento para el firmware y el hardware, lo que afectará negativamente a la ejecución del sistema hasta que se haya completado la recuperación del enlace. Estos errores deben supervisarse exhaustivamente, pues habitualmente afectarán a varios dispositivos de SAN.

Recuerde: A menudo, estos errores se deben a una acción de un técnico de servicio al cliente (CE) al sustituir un dispositivo de SAN. Como parte del mantenimiento que realiza el CE para sustituir o reparar un dispositivo de SAN, puede que el cable de fibra se haya desconectado temporalmente. Si el canal de fibra está desconectado, la hora y la duración del error deben corresponder al momento en el que se ha realizado la actividad de servicio.

Errores comunes de dispositivos de SAN

Se pueden emitir varios mensajes específicos de SAN cuando sufra problemas con los dispositivos de SAN del agente de almacenamiento.

Consulte el apartado Tabla 16 para conocer los errores generados para dispositivos de SAN.

Tabla 16. Errores comunes de dispositivos de SAN

Error	Explicación
ANR8302E Error de E/S en la unidad *TSMDRIVE01* (*/dev/mt9*) (OP=*WRITE*, Número de error=*5*, CC=*205*, KEY=*FF*, ASC=*FF*, ASCQ=*FF*, SENSE=***NONE****, Descripción=*Error SCSI general*). Consulte el apéndice D del manual de mensajes para conocer la acción apropiada.	Este mensaje se emite en ocasiones para los errores del dispositivo de SAN. El CC=205 informa de que el controlador de dispositivo detecta un error en un adaptador SCSI. Si un dispositivo conectado a SAN se encuentra con una reiniciación de un enlace provocada por la pérdida del enlace, se devuelve al controlador del dispositivo como error de adaptador SCSI. La causa subyacente de este error es el evento que ha ocasionado la reinicialización del enlace al perderse éste. La vía de acceso para este dispositivo debería actualizarse en ONLINE=NO emitiendo el mandato **UPDATE PATH**. No establezca la vía de acceso en ONLINE=YES hasta que haya identificado y corregido la causa de la reinicialización del enlace.
ANR8957E: *mandato*: la detección automática está desactivada y el número de serie del que informa la biblioteca no coincide con el número de serie de la definición de biblioteca.	La correlación de dispositivos de SAN de IBM Spectrum Protect ha encontrado una ruta para la biblioteca que indica un número de serie diferente de la definición de IBM Spectrum Protect actual para la biblioteca. El parámetro **AUTODETECT** se definió en NO para el mandato que evitó que el servidor actualizase el número de serie para la biblioteca. Determine la nueva vía de acceso y emita el mandato **UPDATE PATH** para corregir este error.

Tabla 16. Errores comunes de dispositivos de SAN (continuación)

Error	Explicación
ANR8958E: *mandato*: la detección automática está inactiva y el número de serie reportado por la unidad no coincide con el número de serie de la definición de la unidad.	La correlación de dispositivos de SAN de IBM Spectrum Protect ha encontrado una vía de acceso para una unidad que notifica un número de serie diferente de la definición de IBM Spectrum Protect actual para dicha unidad. El parámetro AUTODETECT se ha establecido en NO para el mandato, lo que impide que el servidor actualice el número de serie de esa unidad. Determine la nueva vía de acceso y emita el mandato **UPDATE PATH** para corregir este error.

Tabla 16. Errores comunes de dispositivos de SAN (continuación)

Error	Explicación
ANR8963E: No se ha podido encontrar una vía de acceso que coincida con el número de serie definido para la unidad *nombre_unidad* en la biblioteca *nombre_biblioteca*	La correlación de dispositivos de SAN no puede encontrar un dispositivo de SAN que se haya definido anteriormente en el servidor. La causa más habitual para esto es que el dispositivo en sí mismo se eliminó o sustituyó en la SAN. Es posible que los siguientes pasos resuelvan este error: • Dispositivo eliminado Si se ha eliminado el dispositivo de la SAN, suprima las definiciones de servidor que hacen referencia a este dispositivo. Emita el mandato `QUERY PATH F=D` para determinar las vías de acceso que hacen referencia al dispositivo. A continuación, emita el mandato **DELETE PATH** para eliminar estas vías de acceso. • Dispositivo sustituido Si se ha sustituido un dispositivo por otro dispositivo nuevo debido a una tarea de mantenimiento o a una actualización, siga estos procedimientos: – Intente no suprimir la unidad o la definición de la vía de acceso de unidad después de sustituir la unidad. – Emita uno de los mandatos de servidor siguientes: - `UPDate DRive <nombre_biblioteca> <nombre_unidad> SERIAL=AUTODetect` Este mandato fuerza los registros del nuevo número de serie en la base de datos del servidor. Puesto que la unidad se ha sustituido, el número de elemento continúa siendo el mismo. - `UPDate PATH <nombre_origen> <nombre_unidad> SRCT=SERVER DESTT=DRIVE LIBRary=<nombre_biblioteca> DEVIce=xxxxx AUTODetect=Yes` Este mandato fuerza los registros del nuevo número de serie en la base de datos. Puesto que la unidad se ha sustituido, el número de elemento continúa siendo el mismo. – Si se ha suprimido la unidad o la vía de acceso de unidad, vuelva a definir esta unidad sustituida nueva. Debe reiniciar el servidor de IBM Spectrum Protect para que la correlación de número/número de serie del elemento de la biblioteca se renueve. Esta correlación sólo tiene lugar durante la inicialización. Emita el mandato **QUERY PATH F=D** para buscar las vías de acceso definidas en el servidor que hacen referencia a este dispositivo; a continuación, emita el mandato siguiente para actualizar la información de la vía de acceso: `UPDATE PATH AUTODetect=Yes`

Tabla 16. Errores comunes de dispositivos de SAN (continuación)

Error	Explicación
ANR8972E: No se encuentra el número de elemento para la unidad *nombre de unidad* en la biblioteca *nombre de biblioteca*	Si el parámetro **ELEMent** se establece en AUTODetect al definir la unidad, IBM Spectrum Protect obtiene el número de elemento de la unidad de forma automática. No obstante, si la biblioteca no proporciona una correlación entre el número de elemento y el número de serie, se emite este mensaje. Lleve a cabo los siguientes pasos para corregir el error: 1. Determine el número de elemento de esta unidad de cintas. 2. Emita el mandato **UPDATE DRIVE** para actualizar el número de elemento del dispositivo.

AIX Linux Para ayudar con la determinación de los problemas, puede utilizar el módulo `dsmsanlist` para obtener información sobre los dispositivos en una red de área de almacenamiento (SAN). El módulo `dsmsanlist` está instalado de forma predeterminada cuando el servidor de IBM Spectrum Protect o el agente de almacenamiento de IBM Spectrum Protect está instalado.

Conceptos relacionados:

"Errores de correlación de dispositivos de SAN" en la página 204

Consejos y sugerencias de la correlación de dispositivos de SAN

Tanto el descubrimiento como la correlación de dispositivos de SAN son compatibles con Windows, AIX y Linux (excepto Linux zSeries).

Los siguientes elementos ilustran las ventajas de la detección y de la correlación de dispositivos de SAN de IBM Spectrum Protect:

IBM Spectrum Protect puede visualizar todos los dispositivos en la SAN
El mandato de servidor **QUERY SAN** muestra todos los dispositivos que el servidor puede ver mediante los adaptadores de bus de host de canal de fibra (HBA) instalados en el sistema. Los parámetros que se muestran son el tipo de dispositivo, el nombre del proveedor, el nombre del modelo del producto, el número de serie y el nombre del dispositivo. Si se ha especificado `FORMAT=DETAIL` para la consulta, se visualiza información adicional como, por ejemplo, World Wide Name (WWN), puerto, bus, destino y LUN. Esta información le ayudará a identificar todos los dispositivos de cinta, de disco y del Transportador de datos de la SAN. Para AIX, el transportador de datos no aparece.

IBM Spectrum Protect puede actualizar la vía de acceso de dispositivo automáticamente cuando cambia una vía de acceso de dispositivo
IBM Spectrum Protect no requiere enlace permanente a los dispositivos que ve mediante HBA. En lugar de ello, el servidor utiliza SNIA (Storage Networking Industry Association) HBAAPI para descubrir y obtener el número de serie de todos los dispositivos de la SAN. También puede determinar la vía de acceso de cada dispositivo. Comparando un número de serie de dispositivo registrado en la base de datos de IBM Spectrum Protect con el número de serie obtenido del dispositivo en tiempo real, se detecta un cambio en una ruta del dispositivo. Si la vía de acceso ha cambiado, el descubrimiento de SAN obtiene automáticamente la nueva

vía de acceso del dispositivo. La base de datos de IBM Spectrum Protect también se actualiza con la nueva información de la vía de acceso.

La biblioteca de derivadores HBAAPI es el derivador que utiliza el servidor para comunicarse con el SNIA HBAAPI. La biblioteca de ajustadores HBAAPI está instalada en el mismo directorio que el archivo ejecutable de IBM Spectrum Protect (a menos que se proporcione la vía de acceso completa). La siguiente lista muestra los archivos del derivador HBA que se incluyen con el paquete del servidor (excepto en AIX):

- Windows `hbaapi.dll`
- AIX `/usr/lib/libhbaapi.a` (suministrado por AIX con instalación HBAAPI)
- Linux 32-bit: `libhbaapi32.so`
- Linux 64-bit: `libhbaapi64.so`

Si alguno de estos archivos no está presente, se visualizará el mensaje "ANR1791W La biblioteca de ajustadores HBAAPI xxxxxxxxx no se ha podido cargar o no se encuentra".

Desactivación de la correlación de dispositivos de SAN:

Ocasionalmente, debe desactivar la correlación de dispositivos SAN para solucionar un problema o para identificar un problema cuando esté solucionando problemas de los dispositivos.

Acerca de esta tarea

Realice el paso siguiente para desactivar la correlación de dispositivos y el descubrimiento de dispositivos de SAN:

Procedimiento

Emita el mandato de servidor **setopt SANDISCOVER OFF**. Los mandatos **setopt SANDISCOVERY** se pueden emitir todas las veces que sea necesario.

Consejo: Otro modo de desactivar/activar el descubrimiento de SAN es especificar la siguiente opción en el archivo `dsmserv.opt`:

SANDISCOVERY OFF desactiva el descubrimiento de SAN.

SANDISCOVERY ON activa el descubrimiento de SAN.

SANDISCOVERY ON es el valor predeterminado para plataformas AIX, Linux y Windows.

Información específica de la plataforma:

Cuando trabaje en la asignación de dispositivos SAN, es importante que conozca información específica de su plataforma.

AIX El mandato **QUERY SAN** no mostrará dispositivos de gateway porque éstos no aparecen en AIX.

Linux Existen bibliotecas, herramientas y otros elementos por separado para RHEL3U3. Para ejecutarlos, también debe instalar un módulo de kernel ioctl de Emulex, además del controlador de Emulex. Asegúrese de cargar el controlador de Emulex antes de cargar el módulo ioctl.

Consejo: Consulte la lista de HBA que reciben soporte y los niveles de controlador necesarios para cada sistema operativo.

Errores de correlación de dispositivos de SAN

Los errores que se producen con más frecuencia durante la correlación de dispositivos SAN pueden deberse al descubrimiento de la SAN, al funcionamiento incorrecto del dispositivo de SAN, a bibliotecas no válidas y otros problemas relacionados con la SAN.

ANR1745I: No se pueden detectar los dispositivos de SAN. La función está ocupada.

Este mensaje de error aparece si hay otro descubrimiento de SAN activo.

El servidor no puede realizar el descubrimiento de SAN. Vuelva a intentarlo después de que se haya completado el descubrimiento de SAN.

ANR1786W, ANR1787W o ANR1788W

Es posible que reciba mensajes de error ANR1786W, ANR1787W o ANR1788W cuando se produzca un problema con un descubrimiento SAN. Los siguientes tres mensajes suelen indicar que la biblioteca HBAAPI no funciona con normalidad:

- ANR1786W HBAAPI no puede obtener el nombre del adaptador.
- ANR1787W No se puede abrir el adaptador *nombre_adaptador*.
- ANR1788W No se pueden obtener los atributos del adaptador *nombre_adaptador*.

Si como resultado el servidor no puede realizar el descubrimiento de SAN, vaya al Portal de soporte para comprobar que el controlador del adaptador de bus de host (HBA) está actualizado y al nivel soportado.

ANR1789W La obtención de la asignación de destino HBA ha fallado.

El mensaje de error ANR1789W es el error HBAAPIn más común en la SAN.

"La obtención de la asignación de destino HBA ha fallado" significa que el HBA ha encontrado un error al recopilar información de asignación de dispositivos enviando varios mandatos SCSI.

Verifique que todos los dispositivos SAN funcionan correctamente (por ejemplo, es posible que una SAN Data Gateway se haya colgado y tenga que reiniciarse). Si todos los dispositivos funcionan, verifique que el firmware del dispositivo en la SAN y el controlador HBA estén en los niveles adecuados. Si como resultado el servidor no puede realizar el descubrimiento de SAN, vaya al Portal de soporte para comprobar que el controlador HBA esté actualizado y al nivel soportado.

Consejo: Para los dispositivos de cinta de IBM, asegúrese de que se ha instalado el firmware más actual. El firmware anterior a 4772 para los dispositivos de cintas de IBM 3580 produce problemas con Qlogic HBAAPI.

ANR1790W El descubrimiento de SAN ha fallado.

El mensaje de error ANR1790W es un mensaje general que indica que la función HBAAPI ha fallado y no puede realizar un descubrimiento SAN.

Verifique que todos los dispositivos SAN funcionan correctamente (por ejemplo, es posible que una SAN Data Gateway se haya colgado y tenga que reiniciarse). Si

todos los dispositivos funcionan, verifique que el firmware del dispositivo en la SAN y el controlador HBA estén en los niveles adecuados.

Consejo: Para los dispositivos de cinta de IBM, asegúrese de que se ha instalado el firmware más actual. El firmware anterior a 4772 para los dispositivos de cintas de IBM 3580 produce problemas con Qlogic HBAAPI.

ANR1791W La biblioteca de ajustadores HBAAPI xxxxx no se ha podido cargar o no se encuentra

El servidor utiliza la biblioteca de ajustadores HBAAPI para comunicarse con SNIA HBAAPI.

Las bibliotecas de ajustadores HBAAPI se encuentran en el mismo directorio que el archivo ejecutable de IBM Spectrum Protect (a menos que se dé la vía de acceso completa como se muestra más adelante). La siguiente lista muestra los archivos de ajustadores HBA que se suministran con el paquete de servidores (excepto en AIX y Linux zSeries). El mensaje de error ANR1791W indica que el archivo de ajustadores HBAAPI falta o que IBM Spectrum Protect no lo ha podido cargar. Compruebe que el archivo de ajustadores se encuentre en el mismo directorio que el archivo ejecutable de IBM Spectrum Protect. Los archivos de las bibliotecas de ajustadores de HBAAPI se muestran en la siguiente lista:

- Windows `hbaapi.dll`
- AIX `/usr/lib/libhbaapi.a` (suministrado por AIX con instalación HBAAPI)
- Linux 32-bit: `libhbaapi32.so`
- Linux 64-bit: `libhbaapi64.so`

El resultado es que el servidor no puede realizar el descubrimiento de SAN.

ANR1792W La biblioteca de proveedores HBAAPI no se ha podido cargar o no se encuentra.

El mensaje de error ANR1792W indica que el archivo de la biblioteca del proveedor no se ha podido cargar. Verifique la validez de los archivos de la biblioteca.

Los sistemas AIX o Linux (excepto Linux zSeries) almacenan sus bibliotecas HBAAPI en la ubicación especificada por el archivo `/etc/hba.conf`. Los archivos de Windows se almacenan en el directorio `C:\winnt\system32` . A continuación se muestran ejemplos de archivos de biblioteca de proveedor:

- `C:\winnt\system32\qlsdm.dll` (archivo QlLogic de Windows)
- `/usr/lib/libHBAAPI.a` (archivo Emulex de AIX)
- `/usr/lib/libqlsdm.so` (archivo Qlogic de Linux)
- `/usr/lib/libemulexhbaapi.so` (archivo de 32 bits Emulex de Linux)
- `/usr/lib64/libemulexhbaapi.so` (archivo de 64 bits Emulex de Linux)

El resultado es que el servidor no puede realizar el descubrimiento de SAN.

ANR1793W El descubrimiento de SAN de IBM Spectrum Protect no está admitido en esta plataforma o esta versión de SO

El mensaje de error ANR1793W sólo se muestra si IBM Spectrum Protect intenta realizar una asignación de dispositivos SAN o una operación de descubrimiento de

dispositivos en un sistema operativo no admitido. Los siguientes sistemas operativo no son compatibles con la correlación del dispositivo SAN o el descubrimiento del dispositivo:

- Windows 2003 de 64 bits
- Las versiones de AIX distintas de 52L o 53A. Para el soporte para asignación de dispositivos SAN y descubrimiento de dispositivos en AIX es necesario utilizar la versión 52L (nivel de conjunto de archivos 5.2.0.50), 53A (nivel de conjunto de archivos 5.3.0.10) o una superior.

El resultado es que el servidor no puede realizar el descubrimiento de SAN.

AmNR1794W El descubrimiento de SAN de IBM Spectrum Protect está desactivado mediante las opciones

El mensaje de error ANR1794W indica que el descubrimiento de SAN en el servidor está desactivado.

El descubrimiento de SAN puede desactivarse o activarse emitiendo los mandatos de servidor siguientes:

setopt SANDISCOVERY OFF y setopt SANDISCOVERY PASSIVE
Estos dos mandatos inhabilitan el descubrimiento de SAN. El servidor no puede corregir la vía de acceso del dispositivo automáticamente si la vía de acceso se ha cambiado. Este mandato sólo tiene que emitirse una vez.

La diferencia entre los dos mandatos es que **SANDISCOVERY OFF** sondea el dispositivo y marca la vía de acceso inactiva como fuera de línea. **SANDISCOVERY PASSIVE** no sondea el dispositivo ni marca la vía de acceso inactiva fuera de línea.

setopt SANDISCOVERY ON
Este mandato activa el descubrimiento de SAN. El mandato **SETOPT SANDISCOVERY ON** se puede emitir todas las veces que sea necesario.

Otra manera de desactivar/activar el descubrimiento de SAN es poner la opción siguiente en el archivo `dsmserv.opt`:

SANDISCOVERY OFF o SANDISCOVERY PASSIVE
Estos dos mandatos pueden inhabilitar el descubrimiento de SAN.

SANDISCOVERY ON
Este mandato activa el descubrimiento de SAN.

AIX Linux Windows **SANDISCOVERY** está configurado de forma predeterminada como ON.

Vaya al Portal de soporte para comprobar el nivel de soporte de plataforma, proveedor de HBA y nivel de controlador antes de establecer **SANDISCOVERY** ON para habilitar el descubrimiento de SAN.

AIX Linux Para ayudar con la determinación de los problemas, puede utilizar el módulo `dsmsanlist` para obtener información sobre los dispositivos en una red de área de almacenamiento (SAN). El módulo `dsmsanlist` está instalado de forma predeterminada cuando el servidor o el agente de almacenamiento está instalado.

ANR2034E QUERY SAN: No se ha encontrado ninguna entrada con este criterio.

El mensaje de error ANR2034E se emite cuando el servidor intenta reunir información de configuración para la SAN y no encuentra nada.

El resultado es que el servidor no puede realizar el descubrimiento de SAN.

A continuación se muestran los posibles motivos para no haber encontrado información sobre la SAN:

- No se admiten el sistema ni el nivel del sistema operativo.
- Éste no es un entorno de SAN.
- Puede que haya un problema con la SAN.
- HBAAPI puede devolver el valor cero del número de HBA en el sistema.
- HBAAPI puede devolver el valor cero del número de dispositivos en el sistema.

Realice las tareas siguientes para buscar la información de configuración de la SAN:

- Compruebe el controlador del HBA de canal de fibra y asegúrese de que esté instalado y activado.
- Compruebe el nivel del controlador de HBA para asegurarse de que está actualizado.
- Utilice el programa de utilidad del proveedor del HBA para comprobar los problemas de enlace de canal de fibra notificados.
- Desinstale y, a continuación, vuelva a instalar el controlador del HBA. Si existe un problema con la configuración del HBA, el controlador de dispositivo o la compatibilidad, el problema se corrige en ocasiones desinstalándolo y volviéndolo a instalar.
- Compruebe la conexión del cable de canal de fibra con el HBA.
- Compruebe la conexión del cable de canal de fibra del HBA con el dispositivo de SAN (conmutador, pasarela de datos u otro dispositivo).
- Compruebe el GBIC (Gigabit Inter-phase Converter).
- En el dispositivo de SAN (conmutador, pasarela de datos u otro dispositivo) intente utilizar otro puerto de destino. En ocasiones, los dispositivos de SAN pueden tener una anomalía de puerto específica.
- Detenga el servidor, reinicie el sistema y reinicie el servidor. Si se han efectuado cambios de configuración de la SAN, en ocasiones el sistema operativo, el controlador de dispositivo o el HBA exigen que se reinicie el sistema para poder comunicarse con la SAN.
- Recicle el puerto de destino en el dispositivo de SAN.
- Recoloque la tarjeta del HBA.
- Vuelva a colocar el HBA.

ANR8226E Error al detectar la versión de la biblioteca HBA-API

El mensaje de error ANR8226E sólo se muestra para AIX.

El servidor ha intentado determinar el nivel del conjunto de archivos devices.common.IBM.fc.hba-api y ha encontrado un error. El mensaje de error ANR8226E indica que se ha producido un error al intentar detectar la versión de conjunto de archivos de la biblioteca HBA-API en AIX.

El resultado es que el servidor no puede realizar el descubrimiento de SAN.

AIX

ANR8227E El conjunto de archivos devices.common.IBM.fc.hba-api no está al nivel requerido.

Debido a problemas en el código HBAAPI de AIX, los niveles mínimos del conjunto de archivos devices.common.IBM.fc.hba-api necesario para el descubrimiento de SAN se muestra en la siguiente lista:

- AIX52 - Necesita 5.2.0.50
- AIX53 - Necesita 5.3.0.10

El servidor ha indicado que el conjunto de archivos devices.common.IBM.fc.hba-api se encuentra en un nivel incompatible con las operaciones de IBM Spectrum Protect. Instale el mantenimiento más reciente para este conjunto de archivos si utiliza dispositivos de SAN.

El resultado es que el servidor no puede realizar el descubrimiento de SAN.

Referencia relacionada:

"Consejos y sugerencias de la correlación de dispositivos de SAN" en la página 202

Faltan dispositivos SAN en la visualización del mandato de servidor QUERY SAN:

Las posibles razones para que el mandato del servidor de **QUERY SAN** no muestre todos los dispositivos, se puede deber a la configuración o a problemas de compatibilidad con el proveedor.

Asegúrese de que la opción del servidor SANDISCOVERY se define como ON.

Renovación de la configuración de la SAN:

Es posible que el mandato de servidor **QUERY SAN** no muestre todos los dispositivos debido a la configuración de la SAN.

Es posible que tenga que renovar la SAN porque la configuración ha cambiado (añadir/eliminar dispositivo) y es preciso actualizar la configuración del sistema.

Actualice la configuración en AIX:

En dispositivos de IBM:
Emita el comando **cfgmgr** para configurar nuevos dispositivos y ver la nueva configuración. El nombre del archivo especial para dispositivos de cinta de IBM (no los dispositivos de IBM Spectrum Protect) es /dev/rmtX para dispositivos de cinta y /dev/smcX para cambiadores de medios.

Consejo: Nombre del archivo especial: /dev/rmt0, /dev/smc0

En los dispositivos IBM Spectrum Protect:
Para actualizar los archivos especiales, utilice **smitty** > **dispositivos** > **Dispositivos de IBM Spectrum Protect** > **Eliminar todos los dispositivos definidos** y, a continuación, **Detectar dispositivos soportados por IBM Spectrum Protect**. El nombre de archivo especial es /dev/mtX para dispositivos de cinta y /dev/lbX para cambiadores de medios.

Consejo: Nombre del archivo especial: `/dev/mt0`, `/dev/lb0`

O también puede volver a instalar el controlador de dispositivos de IBM. El controlador de dispositivo de IBM Spectrum Protect actualiza todos los nombres de archivos especiales actuales.

Actualice la configuración en Windows:

Con Plug and Play, el registro de Windows se actualiza y el nombre del dispositivo puede cambiar sin necesidad de reiniciar el sistema o tener que involucrar al controlador de dispositivo. El servidor de IBM Spectrum Protect detecta el cambio en un nombre de archivo especial y actualiza el nuevo nombre de archivo especial cuando accede a los dispositivos de cinta (durante la inicialización del servidor o el funcionamiento normal). El nombre del dispositivo correcto se actualiza en la base de datos de IBM Spectrum Protect. El nombre de archivo especial es `/dev/mtA.B.C.D` para dispositivos de IBM Spectrum Protect y dispositivos de IBM, y `/dev/lbA.B.C.C` para dispositivos de IBM Spectrum Protect y cambiadores de medios de IBM. El nombre de archivo especia TapeX es solo para unidades de cintas de IBM y ChangerX es solo para cambiadores de medios de IBM.

Consejo: Nombre de archivo especial: `mt0.1.0.0`, `lb0.0.1.0`, `Tape0` y `Changer0`.

Actualice la configuración en Linux:

El adaptador de bus de host (HBA) obtiene la información de configuración más actualizada como resultado de RSCN. En ocasiones, el sistema debe reiniciarse para que pueda recoger los cambios de configuración.

En dispositivos de IBM:

Emita el comando **`lin_taped`** para volver a configurar los dispositivos. La información acerca de los dispositivos se puede recuperar desde el archivo `/proc/scsi/IBMtape` en el caso de los dispositivos de cinta y el archivo `/proc/scsi/IBMchanger` en el de los cambiadores de medios. El nombre de archivo especial es /dev/IBMTapeX para dispositivos de cinta y /dev/IBMChangerX para cambiadores de medios.

Consejo: Nombre de archivo especial: `/dev/IBMTape0`, `/dev/IBMChanger0`

En los dispositivos IBM Spectrum Protect:

Los usuarios pueden emitir autoconf, el script de configuración automática del controlador de dispositivo de IBM Spectrum Protect. Este script reside en el directorio `/opt/tivoli/tsm/devices/bin` (o en el mismo directorio que el archivo `tsmscsi`) para poder configurar dispositivos y todos los nombres de archivo especiales actuales e información de dispositivos. El nombre de archivo especial de dispositivo es `/dev/mtX` para dispositivos de cinta y `/dev/lbX` para cambiadores de medios.

Consejo: Nombre de archivo especial: `dev/tsmscsi/mt0`, `/dev/tsmscsi/lb0`

O también puede volver a instalar el controlador de dispositivos de IBM. El controlador de dispositivo de IBM Spectrum Protect actualiza todos los nombres de archivos especiales actuales.

Con el controlador de dispositivo de paso a través de Linux para los dispositivos de IBM Spectrum Protect, el controlador de HBA y el controlador genérico deben volverse a cargar para obtener todos los nombres de archivos especiales actuales. Es preciso que ejecute el script autconf para que el controlador de dispositivo de IBM Spectrum Protect pueda crear archivos de configuración (`/dev/tsmscsi/lbinfo` y `/dev/tsmscsi/mtinfo`). Estos archivos los utiliza el servidor de IBM Spectrum Protect para crear el nombres de archivos especiales después de cada descubrimiento de SAN.

32 bits (Linux xSeries)
Asegúrese de que la biblioteca de ajustadores HBAAPI libhbaapi32.so esté en el mismo directorio que `dsmserv.exe` o en el directorio `/opt/tivoli/tsm/server/bin`.

64 bits (Linux pSeries)
Asegúrese de que la biblioteca de ajustadores HBAAPI `libhbaapi64.so` esté en el mismo directorio que `dsmserv.exe` o en el directorio `/opt/tivoli/tsm/server/bin`.

64 bits (Linux zSeries)
Asegúrese de que la biblioteca de ajustadores pseudo-HBAAPI `libhbaapi64.so` esté en el mismo directorio que `dsmserv.exe` o en el directorio `/opt/tivoli/tsm/server/bin`. La biblioteca de ajustadores, `libhbaapi64.so`, es un enlace al archivo `/usr/lib64/libzfcphbaapi.so`.

Resolución de problemas de configuración que originan la ausencia del dispositivo SAN:

Los posibles motivos por los que el mandato de servidor **QUERY SAN** no muestra todos los dispositivos puede ser debido a un problema de configuración con el hardware de HBA, el nivel de controlador de HBA o el nivel del sistema operativo.

Acerca de esta tarea

Siga estos pasos para corregir los problemas de configuración:

Procedimiento

1. Vaya al Portal de soporte. Verifique el nivel de soporte de la plataforma, el proveedor o el nivel del controlador para asegurarse de que el nivel del controlador HBA y el nivel del sistema operativo sean compatibles y se admitan en IBM Spectrum Protect para el descubrimiento de SAN.
2. Utilice el programa de utilidad del proveedor de HBA para comprobar si el HBA puede detectar el dispositivo. Si el HBA no detecta el dispositivo, puede que el dispositivo no esté conectado. Compruebe el cable de canal de fibra o el cable SCSI. Si el HBA detecta el dispositivo, compruebe la versión del controlador de HBA. Esta versión del controlador puede tener problemas con la API del HBA.
3. AIX Linux Utilice el módulo `dsmsanlist` para obtener información sobre los dispositivos en una red de área de almacenamiento (SAN). El módulo `dsmsanlist` está instalado de forma predeterminada cuando el servidor de IBM Spectrum Protect o el agente de almacenamiento de IBM Spectrum Protect está instalado.

Verificación del soporte de proveedor para cualquier dispositivo concreto de la SAN:

Es posible que muchos dispositivos o combinaciones de dispositivos no estén admitidos en una determinada red de área de almacenamiento (SAN). Estas limitaciones están relacionadas con la obtención de la certificación que deben adquirir los proveedores para los dispositivos que utilizan protocolo de canal de fibra.

Respecto a un dispositivo determinado, verifique con el proveedor del dispositivo si éste es un dispositivo admitido que puede utilizarse en un entorno de SAN. El soporte de proveedor incluye todo el hardware asociado con la SAN, lo que supone verificar con los proveedores que este dispositivo esté admitido por los HBA, concentradores, pasarelas y conmutadores que conforman la red SAN.

Consejos y sugerencias sobre operaciones de archivador NDMP a IBM Spectrum Protect

IBM Spectrum Protect se establece de forma predeterminada en el puerto de control NDMP (network data management protocol) estándar de 10000. Si otra aplicación está utilizando este puerto (como un segundo servidor de IBM Spectrum Protect), todas las operaciones de archivador a servidor fallan.

Para impedir conflictos con otras aplicaciones, utilice la opción de servidor `NDMPCONTROLPORT` para especificar un puerto diferente para el servidor.

Durante las operaciones de archivador a servidor, IBM Spectrum Protect utilizará los siguientes elementos:

- Hasta dos puertos TCP/IP adicionales.
- Un puerto de control que se utiliza internamente por IBM Spectrum Protect durante las operaciones de copia de seguridad y de restauración.
- Un puerto de datos durante las operaciones de copia de seguridad de NDMP a una agrupación de almacenamiento nativa de IBM Spectrum Protect.

El puerto de datos es efímero y se adquiere al principio de las operaciones de copia de seguridad de NDMP en un grupo de almacenamiento nativo de IBM Spectrum Protect. Si un puerto no está disponible, se emite un mensaje de error y la copia de seguridad de los dispositivos NAS en grupos nativos de IBM Spectrum Protect no será posible. Para evitar conflictos con otras aplicaciones, puede controlar qué puerto se adquiere para uso como puerto de datos durante operaciones de copia de seguridad de NDMP mediante la configuración de las opciones de servidor `NDMPPORTRANGELOW` y `NDMPPORTRANGEHIGH`. Un puerto de datos no es necesario para el servidor de IBM Spectrum Protect para restauraciones NAS desde grupos nativos de IBM Spectrum Protect.

Problemas acerca del cortafuegos con copia de seguridad y restauración de archivador NDMP a servidor IBM Spectrum Protect

Un cortafuegos puede impedir que el servidor de archivos NAS (network-attached storage) entre en contacto con el servidor de IBM Spectrum Protect en el puerto de datos adquirido durante las operaciones de copia de seguridad de NAS a una agrupación de almacenamiento nativa. Si debe modificar el puerto de datos que selecciona el servidor de IBM Spectrum Protect, utilice las opciones de servidor `NDMPPORTRANGELOW` y `NDMPPORTRANGEHIGH`.

Un cortafuegos puede impedir que el servidor de IBM Spectrum Protect entre en contacto con un servidor de archivos NAS en el puerto de datos configurado durante las operaciones de restauración NAS desde un grupo de almacenamiento nativo. Si un cortafuegos impide que IBM Spectrum Protect pueda acceder al servidor de archivos NAS, la conexión de salida de IBM Spectrum Protect fallará.

Resolución de problemas de los dispositivos SCSI

Las unidades de cinta y las bibliotecas pueden pasar a IBM Spectrum Protect información sobre el error encontrado. Esta información se notifica en uno o más de los mensajes.

Si se han emitido los mensajes ANR8300, ANR8301, ANR8302, ANR8303, ANR8943 o ANR98944, los datos que el IBM Spectrum Protect notifica de estos dispositivos pueden ayudar a determinar los pasos necesarios para resolver el problema. Generalmente, cuando el servidor notifica datos de dispositivos utilizando estos mensajes, el problema suele estar relacionado con el dispositivo, la conexión con el dispositivo o cualquier otro problema relacionado que esté fuera de IBM Spectrum Protect.

Utilizando la información ofrecida en los mensajes ANR8300, ANR8301, ANR8302, ANR8303, ANR8943 o ANR8944 de IBM Spectrum Protect, consulte la información sobre el producto de Mensajes de IBM Spectrum Protect en Mensajes, códigos de retorno y códigos de error. Este apéndice contiene información acerca de los errores estándar que puede notificar cualquier dispositivo SCSI. También puede utilizar esta información con la documentación que proporcione el proveedor para el hardware a fin de que le resulte más sencillo determinar la causa y la resolución del problema.

Resolución de errores de un volumen de medios secuenciales (cinta) mediante los mensajes ANR0542W o ANR8778W

Los problemas que se producen con los volúmenes de medios secuenciales se pueden detectar a través de los mensajes de error ANR0542W yANR8778W.

ANR0542W Ha fallado la recuperación o la restauración para la sesión *número_sesión* del nodo *nombre_nodo*; no se puede acceder al medio de almacenamiento.

El mensaje de error ANR0542W suele estar relacionado con una problema relativo a la unidad o la conexión con la unidad que se seleccionó para leer este volumen de cinta.

Para verificar si IBM Spectrum Protect puede acceder a este volumen, lleve a cabo los pasos siguientes:

- Emita el mandato `QUERY LIBVOL` *`nombre_biblioteca nombre_volumen`*.
- Para una biblioteca 349X, emita el mandato `mtlib -l /dev/lmcp0 -qV` *`nombre_volumen`*. El dispositivo suele ser `/dev/lmcp0`, pero si es diferente, sustituya el dispositivo de punto de control del gestor de bibliotecas correcto.

Los siguientes pasos podrían resolver posiblemente este problema:

1. Si mtlib no notifica este volumen, lo más probable es que este volumen esté fuera de la biblioteca. En tal caso, vuelva a colocar el volumen en la biblioteca.

2. Si el volumen no es el indicado por QUERY LIBVOL, el servidor no tiene información sobre este volumen en la biblioteca. Emita el mandato **CHECKIN LIBVOL** para sincronizar el inventario de biblioteca en el servidor con los volúmenes que están en la biblioteca de cintas.
3. Si los dos mandatos notifican correctamente este volumen, la causa probablemente sea un error de hardware permanente o intermitente. Podría ser un error de la propia unidad o un error de la conexión con la unidad. En cualquiera de los dos casos, revise las anotaciones de errores del sistema y póngase en contacto con el proveedor del hardware para resolver el problema.

ANR8778W El volumen reutilizable ha pasado al estado privado para impedir que se acceda a él.

Revise los mensajes de las anotaciones de actividades para determinar la causa del problema que afecta a este volumen reutilizable. Revise también las anotaciones de errores del sistema y las anotaciones de errores de los dispositivos para obtener una indicación sobre si ha habido un problema con la unidad que se ha utilizado para intentar grabar datos en este volumen reutilizable.

Si este error lo ha producido una unidad que requiere limpieza o algún otro problema específico de hardware que se ha resuelto, los volúmenes cuyo estado se estableció como privado como resultado de esta operación pueden restablecerse al estado inicial emitiendo el mandato AUDIT LIBRARY *nombre_biblioteca*.

Apéndice A. Obtención de información de pila de llamadas desde un archivo del núcleo

Utilice el shell de script gt de muestra que se suministra aquí para obtener la pila de llamadas de cada hebra que se esté ejecutando en un archivo de núcleo.

Los parámetros de entrada son la ruta/nombre del archivo ejecutable (valor predeterminado ./dsmserv) y la ruta/nombre del archivo de núcleo (valor predeterminado ./dsmcore). El archivo de salida es `dsm_gdb.info`.

Restricción: Los archivos `dsm_gdb.cmd` and `dsm_gdb.info` se sobrescribirán cuando se ejecute este script.

```
#!/bin/ksh
#
# Si ve el siguiente error:
#   ./dsm_gdb.cmd:9: error en archivo de mandatos fuente:
# No se ha cargado ninguna tabla de símbolos. Utilice el mandato "file".
#   en ese caso, comente la línea en la que se imprime buildStringP
#
# si ve otros errores, deberá encargarse de su resolución...
exe=${1:-"./dsmserv"} # get parm 1 (vía acceso/nombre archivo ejecutable),
set default
core=${2:-"./dsmcore"} # get parm 2 (vía acceso/nombre archivo de núcleo),
                       # establecer predeterminado
echo " "
# buscar el archivo ejecutable... salir si no se encuentra
if [[ -f $exe ]]; then
echo "using executable file:" $exe
else
echo "didn't find executable file ("$exe") ... exiting"
exit
fi
# buscar el archivo de núcleo, si no se encuentra,
# buscar ./core ... salir si no se encuentra
if [[ -f $core ]]; then
echo "using core file:" $core
else
if [[ -f ./core ]]; then
echo "didn't find core file ("$core") but found ./core ... renaming to" $core
mv ./core $core
echo "using core file:" $core
else
echo "didn't find core file ("$core") ... exiting"
exit
fi
fi
echo " "
# establecer que el archivo de mandatos gdb obtenga la información de hebra
nl="\0134\0156"    # códigos octales para \n (así echo no interpretará que es \n)
echo "# dsm gdb command file" >|dsm_gdb.cmd
echo "define doit" >>dsm_gdb.cmd
echo "info registers" >>dsm_gdb.cmd # mostrar valores de registro
echo "echo" $nl >>dsm_gdb.cmd
echo "where" >>dsm_gdb.cmd # mostrar rastreo de la función
echo "echo" $nl"====================================="$nl >>dsm_gdb.cmd
echo "end" >>dsm_gdb.cmd
echo "echo" $nl"====================================="$nl$nl >>dsm_gdb.cmd
echo "x/s buildStringP" >>dsm_gdb.cmd
echo "echo" $nl"====================================="$nl$nl >>dsm_gdb.cmd
echo "info threads" >>dsm_gdb.cmd # mostrar información de hebra
```

```
echo "echo" $nl"====================================="$nl >>dsm_gdb.cmd
echo "thread apply all doit" >>dsm_gdb.cmd
echo "quit" >>dsm_gdb.cmd
echo "invocando gdb para obtener información de hebra"
echo "(observar si existen errores)..."
echo "si ve:"
echo ". aviso: las bibliotecas compartidas no se han correlacionado privadamente;
el establecimiento de un punto de interrupción"
echo ". no funcionará hasta que vuelva a ejecutar el programa"
echo "entonces todo es correcto."
echo "si ve:"
echo ". ./dsm_gdb.cmd:x: error en archivo de mandato fuente:"
echo "escriba 'quit', edite este script y lea los comentarios del principio"
gdb -se $exe -c $core -x ./dsm_gdb.cmd >|dsm_gdb.info
rm dsm_gdb.cmd   # se ha completado
exit
```

Apéndice B. Ejecute el programa de utilidad tsmdiag

Puede diagnosticar los problemas de un servidor de IBM Spectrum Protect ejecutando el programa de utilidad tsmdiag en el sistema donde está instalado el servidor de IBM Spectrum Protect. Después de recopilar los datos de diagnóstico, puede enviar la información al servicio de soporte de software de IBM.

Procedimiento

Para ejecutar el programa de utilidad tsmdiag, siga estos pasos:

1. AIX Linux Cambie los permisos del directorio `tsmdiag` ejecutando el mandato siguiente:

   ```
   chmod -R 757 /opt/tivoli/tsm/server/bin/tsmdiag
   ```

2. Emita el mandato **tsmdiag** desde el directorio siguiente:

   - AIX Linux Utilizando una instancia del ID de usuario de DB2, debe emitir el mandato **tsmdiag** desde el directorio `/opt/tivoli/tsm/server/bin/tsmdiag`.
   - Windows Utilizando un ID de administrador, debe emitir el mandato **tsmdiag** desde el directorio `\server\tsmdiag`.

   Por ejemplo, el siguiente mandato recopila un conjunto predeterminado de archivos de información de diagnóstico desde un servidor de IBM Spectrum Protect en un host local. Este mandato lo ejecuta un administrador con el nombre admin y una contraseña de administrador admin01 en un servidor de IBM Spectrum Protect. Este servidor se ejecuta en el puerto TCP/IP 1501 de un host local.

   ```
   tsmdiag -id admin -pa admin01 -tcpport 1501
   ```

3. Obtenga el archivo de resultados desde el directorio siguiente:

   - AIX Linux `/opt/tivoli/tsm/server/bin/tsmdiag/results/tsmdiag_results<year>-<month>-<day>-<hour>-<minute>-<second>.tar`
   - Windows `C:\Program Files\tivoli\tsm\server\tsmdiag\results\tsmdiag_results<year>-<month>-<day>-<hour>-<minute>-<second>.zip`

4. Envíe el archivo de resultados con el informe de problemas al servicio de soporte de software de IBM.

Mandatos tsmdiag de ejemplo

El mandato siguiente se conecta a un servidor de IBM Spectrum Protect denominado MYSERVER en el puerto TCP/IP 1501. Cuando un administrador de DB2 con el nombre admin ejecuta el mandato siguiente, se recopila un conjunto predeterminado de archivos de información de diagnóstico. También se recopila información de diagnóstico sobre el rendimiento del servidor MYSERVER.

```
tsmdiag -id admin -pa admin01 -tcpport 1501 -servername MYSERVER -performance
```

El mandato siguiente se conecta a un servidor de IBM Spectrum Protect en el puerto TCP/IP predeterminado 1500. Cuando un administrador con el nombre admin ejecuta el mandato siguiente, éste recopila un conjunto predeterminado de archivos de información de diagnóstico. Este mandato también proporciona

resultados de los mandatos del servidor de IBM Spectrum Protect **SHOW** y alguna información de diagnóstico acerca del estado del servidor de IBM Spectrum Protect.

```
tsmdiag -id admin -pa admin01 -hang
```

Opciones del programa de utilidad tsmdiag

El programa de utilidad tsmdiag puede ayudarle a diagnosticar problemas con un componente del servidor de IBM Spectrum Protect. Cuando ejecuta el programa de utilidad, puede especificar opciones que determinan el tipo de información de diagnóstico proporcionada.

Puede especificar las siguientes opciones para emitir el mandato **tsmdiag**:

id *adminName*
: El ID del administrador o del usuario root del servidor en el que se ejecuta el mandato **tsmdiag**. Esta opción es obligatoria.

-pa *adminPwd*
: La contraseña del ID de administrador o de usuario root. Esta opción es obligatoria.

-tcpserveraddress *ipAddress*
: Especifica el nombre o la dirección TCP/IP del servidor en el que se ejecuta el mandato **tsmdiag**. La opción es opcional. El valor predeterminado es `localhost`.

-tcpport *portNumber*
: Especifica el puerto TCP/IP del servidor en el que se ejecuta el mandato **tsmdiag**. Esta opción es opcional. El valor predeterminado es `1500`.

AIX Linux **-servername**
: El nombre del servidor en el que se ejecuta el mandato **tsmdiag**. Esta opción es opcional. El valor predeterminado es `SERVER1`.

-crash Especifica si se ha de informar en caso de que falle el servidor. Esta opción es opcional. El valor predeterminado es `off`.

-dbcorrupt
: Especifica si se ha de informe en caso de que la base de datos esté dañada. Esta opción es opcional. El valor predeterminado es `off`.

-dbgrowth
: Especifica si se ha de informar en caso de un crecimiento excesivo de la base de datos en el servidor. Esta opción ejecuta el script `serverReorgInfo.pl` y el script `tsmdiag_dedup_stats.pl`, el cual genera información de diagnóstico adicional. El script `serverReorgInfo.pl` tarda 1 hora en ejecutarse. Esta opción es opcional. El valor predeterminado es `off`.

-hang Especifica si se ha de informar en caso de que se cuelgue el servidor. Esta opción es opcional. El valor predeterminado es `off`.

-performance
: Especifica si se ha de informar si se producen problemas de rendimiento en el servidor. Esta opción ejecuta el script `tsmdiag_sysmonv6.pl`, el cual genera información de diagnóstico adicional. El script `tsmdiag_sysmonv6.pl` puede tardar hasta 1,5 horas en ejecutarse. Esta opción es opcional. El valor predeterminado es `off`.

-v Especifica que la salida de informes se genera en formato detallado. Esta opción es opcional. El valor predeterminado es `off`.

-? Especifica la información de uso para el programa de utilidad tsmdiag. Si emite el mandato `tsmdiag ?` se muestra una lista de las opciones anteriores.

Apéndice C. Códigos de retorno de IBM Global Security Kit

El servidor y el cliente utilizan el proceso de IBM Global Security Kit (GSKit) para SSL (Secure Sockets Layer) entre el servidor y el cliente de archivado y copia de seguridad. Algunos mensajes que se emiten para el proceso de SSL incluyen códigos de retorno de GSKit.

GSKit se instala o actualiza automáticamente durante la instalación de IBM Spectrum Protect y proporciona las bibliotecas siguientes:

- SSL de GSKit
- API de gestión de claves GSKit
- IBM Crypto for C (ICC)

Los informes del programa de utilidad tsmdiag notifican el nivel de GSKit que se ha instalado en el sistema o puede utilizar uno de estos métodos:

- Para Windows, emita los mandatos siguientes:

  ```
  regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8\"
  notepad gskitinfo.txt
  ```

  PRECAUCIÓN:
  Puede dañar el registro del sistema si utiliza regedit de forma incorrecta.
- Para el servidor AIX de 64 bits, emita el siguiente mandato desde la línea de mandatos: `gsk8ver_64`

Consulte la Tabla 17 para ver los códigos de retorno SSL de GSKit.

El servidor utiliza la API de gestión de claves GSKit para crear automáticamente la base de datos de gestión de claves y las claves públicas y privadas del servidor. Algunos mensajes que se emiten para este proceso pueden incluir códigos de retorno de GSKit Key Management. Consulte la Tabla 18 en la página 226 para ver los códigos de retorno de gestión de claves.

Tabla 17. Códigos de retorno generales de IBM Global Security Kit SSL

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000000	0	GSK_OK	La tarea se completa correctamente. Lo emite cada llamada de función que se completa correctamente.
0x00000001	1	GSK_INVALID_HANDLE	El entorno o el manejador de SSL no es válido. El manejador especificado no era el resultado de una llamada de función `open()` correcta.
0x00000002	2	GSK_API_NOT_AVAILABLE	La biblioteca de enlace dinámico (DLL) se ha descargado y no está disponible (se produce sólo en sistemas Microsoft Windows.
0x00000003	3	GSK_INTERNAL_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	No hay suficiente memoria disponible para ejecutar la operación.

Tabla 17. Códigos de retorno generales de IBM Global Security Kit SSL (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000005	5	GSK_INVALID_STATE	El manejador tiene un estado no válido para la operación como, por ejemplo, realizar una operación `init()` en un manejador dos veces.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	No se ha encontrado la etiqueta de clave especificada en el archivo de claves.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	No se ha recibido el certificado del socio.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Error de validación del certificado.
0x00000009	9	GSK_ERROR_CRYPTO	Error al procesar el cifrado.
0x0000000a	10	GSK_ERROR_ASN	Error al validar campos ASN en el certificado.
0x0000000b	11	GSK_ERROR_LDAP	Error al establecer la conexión con el registro de usuario.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x0000000d	13	GSK_INVALID_PARAMETER	Parámetro no válido.
0x0000000e	14	GSK_ERROR_UNEXPECTED_INT_EXCEPTION	Parámetro no válido. Informe de este error al servicio de soporte de software de IBM.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000066	102	GSK_KEYFILE_IO_ERROR	Error de E/S al leer el archivo de claves.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	El archivo de claves no tiene un formato interno válido. Vuelva a crear el archivo de claves.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	El archivo de claves tiene dos entradas con la misma clave.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	El archivo de claves tiene dos entradas con la misma etiqueta.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	La contraseña del archivo de claves se utiliza como comprobación de integridad. El archivo de claves se ha dañado o el ID de contraseña es incorrecto.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	La clave predeterminada en el archivo de claves tiene un certificado caducado.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Se ha producido un error al cargar una de las bibliotecas de enlace dinámico GSK. Asegúrese de que GSK se ha instalado correctamente.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Indica que se está intentando establecer una conexión en un entorno GSK después de que se haya establecido `GSK_ENVIRONMENT_ CLOSE_OPTIONS` en `GSK_DELAYED_ ENVIRONMENT_CLOSE` y se ha llamado a la función `gsk_environment_close()`.

Tabla 17. Códigos de retorno generales de IBM Global Security Kit SSL (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	No se han especificado ni la contraseña ni el nombre del archivo stash. El archivo de claves no se ha inicializado.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	No se ha podido abrir el archivo de claves. La vía de acceso se ha especificado de forma incorrecta o los permisos de archivo no han permitido que se abra el archivo.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	No se puede generar un par de claves temporal. Informe de este error al servicio de soporte de software de IBM.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Se ha especificado un objeto de nombre de usuario que no se ha podido encontrar.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Una contraseña utilizada para una consulta LDAP (lightweight directory access protocol) no es correcta.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Un índice de la lista de servidores LDAP de migración tras anomalía no era correcto.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Esta instalación de GSKit no admite modalidad de operación FIPS.
0x0000012d	301	GSK_CLOSE_FAILED	Indica que la solicitud de cierre del entorno GSK no se ha gestionado correctamente. El motivo más probable es que se ha intentado un mandato `gsk_secure_socket*()` después de una llamada a `gsk_close_environment()`.
0x00000191	401	GSK_ERROR_BAD_DATE	La fecha del sistema no se ha establecido en un valor válido.
0x00000192	402	GSK_ERROR_NO_CIPHERS	No se han habilitado SSLv2 ni SSLv3.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	No se ha recibido del socio el certificado necesario.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	El certificado recibido se ha formateado de forma incorrecta.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	El tipo de certificado recibido no se ha admitido.
0x00000196	406	GSK_ERROR_IO	Se ha producido un error de E/S en una operación de lectura o grabación de datos.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	No se encuentra la etiqueta especificada en el archivo de claves.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	La contraseña del archivo de claves especificado es incorrecta. No se puede utilizar el archivo de claves. Es posible también que el archivo de claves esté dañado.

Tabla 17. Códigos de retorno generales de IBM Global Security Kit SSL (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	En un entorno de cifrado limitado, el tamaño de la clave es demasiado largo para que se pueda admitir.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Se ha recibido un mensaje SSL con formato incorrecto de la otra parte.
0x0000019b	411	GSK_ERROR_BAD_MAC	El código de autenticación de mensaje (MAC) no se ha verificado correctamente.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Protocolo SSL no admitido o tipo de certificado no admitido.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	El certificado recibido contenía una firma incorrecta.
0x0000019e	414	GSK_ERROR_BAD_CERT	Se ha recibido un certificado con formato incorrecto del socio.
0x0000019f	415	GSK_ERROR_BAD_PEER	No se ha recibido un protocolo SSL válido del socio.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Informe de este error al servicio de soporte de software de IBM.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	El certificado autofirmado no es válido.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	`read()` ha presentado anomalías. Informe de este error al servicio de soporte de software de IBM.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	`write()` ha presentado anomalías. Informe de este error al servicio de soporte de software de IBM.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	La otra parte ha cerrado el socket antes de que se completara el protocolo.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	El Cipher V2 especificado no es válido.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	El Cipher V3 especificado no es válido.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Informe de este error al servicio de soporte de software de IBM.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Informe de este error al servicio de soporte de software de IBM.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	No se puede crear el manejador. Informe de este error al servicio de soporte de software de IBM.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	la inicialización no se ha realizado. Informe de este error interno al servicio.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	No se puede acceder al registro de usuario especificado al validar un certificado.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	La clave especificada no contenía una clave privada.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Se ha realizado un intento fallido de cargar la biblioteca compartida PKCS11.

Tabla 17. Códigos de retorno generales de IBM Global Security Kit SSL (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	El controlador PKCS #11 no ha podido encontrar la señal especificada por el operador.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	La ranura no contiene ninguna señal PKCS #11.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	El pin/contraseña para acceder a la señal PKCS nº11 no es válido.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	La cabecera SSL recibida no era una cabecera con el formato SSLv2 correcto.
0x000001b2	434	GSK_CSP_OPEN_ERROR	No se puede abrir el proveedor de servicios de cifrado basado en hardware. No se ha especificado correctamente el nombre de CSP o no se ha podido acceder al almacén de certificados de CSP especificado.
0x000001b3	435	GSK_CONFLICTING_ATTRIBUTE_SETTING	Conflicto de establecimiento de atributos entre PKCS11, base de datos de claves CMS y Microsoft Crypto API.
0x000001b4	436	GSK_UNSUPPORTED_PLATFORM	La función solicitada no recibe soporte en la plataforma en la que se ejecuta la aplicación. Por ejemplo, Microsoft Crypto API no recibe soporte en plataformas que no sean Windows 2000.
0x000001b6	438	GSK_ERROR_INCORRECT_SESSION_TYPE	Se ha devuelto un valor incorrecto desde la función de devolución de llamada del tipo restablecer sesión. Sólo se permite GSKit `gsk_sever_session`, `gsk_sever_session_with_cl_auth` o `gsk_sever_session_with_cl_auth_crit`.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	El tamaño del almacenamiento intermedio es negativo o cero.
0x000001f6	502	GSK_WOULD_BLOCK	Se utiliza con E/S sin bloqueo. Consulte la sección sobre no bloqueo para su uso.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 es necesario para `reset_cipher()` y la conexión utiliza SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	No se ha especificado un ID válido para la llamada de la función `gsk_secure_soc_misc()`.
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	La llamada de la función tiene un ID no válido. Este problema también se puede producir al especificar un manejador de entorno cuando debe utilizarse un manejador para una conexión SSL.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	El atributo tiene una longitud negativa, la cual no es válida.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	El valor de enumeración no es válido para el tipo de enumeración especificada.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Lista de parámetros no válida para sustituir las rutinas de caché SID.

Tabla 17. Códigos de retorno generales de IBM Global Security Kit SSL (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Al establecer un atributo numérico, el valor especificado no es válido para el atributo específico que se está estableciendo.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Se han establecido parámetros conflictivos para la validación adicional de certificados.
0x000002c3	707	GSK_AES_UNSUPPORTED	El algoritmo de cifrado AES no recibe soporte.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	PEERID no tiene la longitud correcta.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	El cifrado concreto no se permite cuando la modalidad de funcionamiento FIPS está desactivada.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No se seleccionan cifrados FIPS aprobados en la modalidad de funcionamiento FIPS.
0x00000641	1601	GSK_TRACE_STARTED	El rastreo se ha iniciado satisfactoriamente.
0x00000642	1602	GSK_TRACE_STOPPED	El rastreo se ha detenido satisfactoriamente.
0x00000643	1603	GSK_TRACE_NOT_STARTED	No se ha iniciado ningún archivo de rastreo anteriormente y, por lo tanto, no se puede detener.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	El archivo de rastreo se ha iniciado y, por lo tanto, no se puede reiniciar.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	El archivo de rastreo no se puede abrir. El primer parámetro de `gsk_start_trace()` debe ser un nombre completo de archivo de vía de acceso válido.

Tabla 18. Códigos de retorno de gestión de claves de IBM Global Security Kit

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000000	0	GSK_OK	La tarea se completa correctamente. Este mensaje lo emite cada llamada de función que se completa correctamente.
0x00000001	1	GSK_INVALID_HANDLE	El entorno o el manejador de SSL no es válido. El manejador especificado no era el resultado de una llamada de función open() satisfactoria.
0x00000002	2	GSK_API_NOT_AVAILABLE	La biblioteca de enlace dinámico (DLL) se ha descargado y no está disponible (se produce sólo en sistemas Microsoft Windows).

Tabla 18. Códigos de retorno de gestión de claves de IBM Global Security Kit (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000003	3	GSK_INTERNAL_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	No hay suficiente memoria disponible para ejecutar la operación.
0x00000005	5	GSK_INVALID_STATE	El manejador se encuentra en un estado incorrecto para la operación como, por ejemplo, ejecutar una operación init() en un manejador dos veces.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	No se ha encontrado la etiqueta de clave especificada en el archivo de claves.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	No se ha recibido el certificado del socio.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Error de validación del certificado.
0x00000009	9	GSK_ERROR_CRYPTO	Error al procesar el cifrado.
0x0000000a	10	GSK_ERROR_ASN	Error al validar campos ASN en el certificado.
0x0000000b	11	GSK_ERROR_LDAP	Error al establecer la conexión con el registro de usuario.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000066	102	GSK_KEYFILE_IO_ERROR	Error de E/S al leer el archivo de claves.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	El archivo de claves tiene un formato interno que no es válido. Vuelva a crear el archivo de claves.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	El archivo de claves tiene dos entradas con la misma clave.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	El archivo de claves tiene dos entradas con la misma etiqueta.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_ PASSWORD	La contraseña del archivo de claves se utiliza como comprobación de integridad. El archivo de claves se ha dañado o el ID de contraseña es incorrecto.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	La clave predeterminada en el archivo de claves tiene un certificado caducado.

Tabla 18. Códigos de retorno de gestión de claves de IBM Global Security Kit (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Se ha producido un error al cargar una de las bibliotecas de enlaces dinámicos de GSK. Asegúrese de que GSK se ha instalado correctamente.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Este mensaje indica que se está intentando establecer una conexión en un entorno GSK después de que se haya establecido GSK_ENVIRONMENT_ CLOSE_OPTIONS en GSK_DELAYED_ ENVIRONMENT_CLOSE y se ha llamado a la función gsk_environment_close().
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	No se han especificado ni la contraseña ni el archivo stash por lo que no se ha inicializado el archivo de claves.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	No se ha podido abrir el archivo de claves. La vía de acceso se ha especificado de forma incorrecta o los permisos de archivo no han permitido que se abra el archivo.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	No se puede generar un par de claves temporal. Informe de este error al servicio de soporte de software de IBM.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Se ha especificado un objeto de nombre de usuario que no se ha podido encontrar.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_ CREDENTIALS	Una contraseña utilizada para una consulta LDAP no es correcta.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Un índice de la lista de servidores LDAP de migración tras anomalía no era correcto.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Esta instalación de GSKit no admite modalidad de operación FIPS.
0x0000012d	301	GSK_CLOSE_FAILED	Indica que la solicitud de cierre del entorno GSK no se ha gestionado correctamente. El motivo más probable es que se ha intentado un mandato gsk_secure_socket*() después de una llamada a gsk_close_environment().

Tabla 18. Códigos de retorno de gestión de claves de IBM Global Security Kit (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000191	401	GSK_ERROR_BAD_DATE	La fecha del sistema se ha establecido en un valor que no es válido.
0x00000192	402	GSK_ERROR_NO_CIPHERS	No se han habilitado SSLv2 ni SSLv3.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	No se ha recibido del socio el certificado necesario.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	El certificado recibido se ha formateado de forma incorrecta.
0x00000195	405	GSK_ERROR_UNSUPPORTED_ CERTIFICATE_TYPE	El tipo de certificado recibido no se ha admitido.
0x00000196	406	GSK_ERROR_IO	Se ha producido un error de E/S en una operación de lectura o grabación de datos.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	No se encuentra la etiqueta especificada en el archivo de claves.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	La contraseña del archivo de claves especificado es incorrecta. No se puede utilizar el archivo de claves. Es posible que el archivo de claves esté dañado.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_ FOR_EXPORT	En un entorno de cifrado limitado, el tamaño de la clave es demasiado largo para que se pueda admitir.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Se ha recibido un mensaje SSL con formato incorrecto de la otra parte.
0x0000019b	411	GSK_ERROR_BAD_MAC	El MAC no se ha verificado correctamente.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Protocolo SSL no admitido o tipo de certificado no admitido.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	El certificado recibido contenía una firma incorrecta.
0x0000019e	414	GSK_ERROR_BAD_CERT	Se ha recibido un certificado con formato incorrecto del socio.
0x0000019f	415	GSK_ERROR_BAD_PEER	Se ha recibido del socio un protocolo SSL que no es válido.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Informe de este error al servicio de soporte de software de IBM.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	El certificado autofirmado no es válido.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	Error en read(). Informe de este error al servicio de soporte de software de IBM.

Tabla 18. Códigos de retorno de gestión de claves de IBM Global Security Kit (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	Error en write(). Informe de este error al servicio de soporte de software de IBM.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	La otra parte ha cerrado el socket antes de que se completara el protocolo.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	El Cipher V2 especificado no es válido.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	El Cipher V3 especificado no es válido.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Informe de este error al servicio de soporte de software de IBM.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_ COMBINATION	Informe de este error al servicio de soporte de software de IBM.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_ FAILED	No se ha creado el manejador. Informe de este error al servicio de soporte de software de IBM.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	la inicialización no se ha realizado. Informe de este error interno al servicio.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	No se puede acceder al registro de usuario especificado al validar un certificado.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	La clave especificada no contenía una clave privada.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_ NOTLOADED	Se ha realizado un intento fallido de cargar la biblioteca compartida PKCS11.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_ LABELMISMATH	El controlador PKCS #11 no ha podido encontrar la señal especificada por el operador.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_ NOTPRESENT	La ranura no contiene ninguna señal PKCS #11.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_ BADPASSWORD	El pin/contraseña para acceder a la señal PKCS nº11 es incorrecto.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	La cabecera SSL recibida no era una cabecera con el formato SSLv2 correcto.
0x000001b2	434	GSK_CSP_OPEN_ERROR	No se ha podido abrir el proveedor de servicios de cifrado basado en hardware (CSP). No se ha especificado correctamente el nombre de CSP o no se ha podido acceder al almacén de certificados de CSP especificado.

Tabla 18. Códigos de retorno de gestión de claves de IBM Global Security Kit (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000001b3	435	GSK_CSP_OPEN_ERROR	Se han definido algunos atributos conflictivos para la operación de SSL.
0x000001b4	436	GSK_CSP_OPEN_ERROR	La API de Microsoft Crypto sólo es compatible con Microsoft Windows 2000 con Service Pack 2 aplicado.
0x000001b5	437	GSK_CSP_OPEN_ERROR	El sistema se ejecuta en modalidad IPv6 sin establecer un PEERID.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	El tamaño del almacenamiento intermedio es negativo o cero.
0x000001f6	502	GSK_WOULD_BLOCK	Se utiliza con E/S sin bloqueo. Consulte la sección sobre no bloqueo para su uso.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 es necesario para reset_cipher() y la conexión utiliza SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Se ha especificado un ID que no es válido para la llamada de la función gsk_secure_soc_misc().
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	La llamada de la función tiene un ID que no es válido. Este problema también se puede producir al especificar un manejador de entorno cuando debe utilizarse un manejador para una conexión SSL.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	El atributo tiene una longitud negativa, la cual no es válida.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ ENUMERATION	El valor de enumeración no es válido para el tipo de enumeración especificada.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Lista de parámetros no válida para sustituir las rutinas de caché SID.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_ NUMERIC_VALUE	Al establecer un atributo numérico, el valor especificado no es válido para el atributo específico que se está estableciendo.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_ SETTING	Se han establecido parámetros conflictivos para la validación adicional de certificados.
0x000002c3	707	GSK_AES_UNSUPPORTED	El algoritmo de cifrado AES no recibe soporte.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	PEERID no tiene la longitud correcta.

Tabla 18. Códigos de retorno de gestión de claves de IBM Global Security Kit (continuación)

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	El cifrado concreto no se permite cuando la modalidad de funcionamiento FIPS está desactivada.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No se seleccionan cifrados FIPS aprobados en la modalidad de funcionamiento FIPS.
0x00000641	1601	GSK_TRACE_STARTED	El rastreo se ha iniciado satisfactoriamente.
0x00000642	1602	GSK_TRACE_STOPPED	El rastreo se ha detenido satisfactoriamente.
0x00000643	1603	GSK_TRACE_NOT_STARTED	No se ha iniciado ningún archivo de rastreo anteriormente y, por lo tanto, no se puede detener.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	El archivo de rastreo se ha iniciado y, por lo tanto, no se puede volver a iniciar.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	El archivo de rastreo no se puede abrir. El primer parámetro de gsk_start_trace() debe ser un nombre completo de archivo de vía de acceso válido.

Apéndice D. Funciones de accesibilidad para la familia de productos IBM Spectrum Protect

Las funciones de accesibilidad ayudan a los usuarios con discapacidades, como movilidad restringida o visión limitada, para que puedan utilizar el contenido de las tecnologías de la información satisfactoriamente.

Visión general

La familia de productos de IBM Spectrum Protect incluye las siguientes funciones de accesibilidad:

- Uso sólo con el teclado
- Operaciones que utilizan un lector de pantalla

La familia de productos de IBM Spectrum Protect utiliza el último estándar de W3C, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), para garantizar la conformidad con US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) y Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Para sacar partido de las funciones de accesibilidad, utilice la última versión del lector de pantalla y el último navegador web admitido por el producto.

Se ha añadido accesibilidad a la documentación del producto disponible en IBM Knowledge Center. Las funciones de accesibilidad de IBM Knowledge Center están descritas en la sección de accesibilidad de la ayuda de IBM Knowledge Center (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navegación con teclado

Este producto utiliza teclas de navegación estándar.

Información sobre la interfaz

Las interfaces de usuario no tienen contenido que se actualice entre 2 y 55 veces por segundo.

Las interfaces de usuario web se basan en hojas de estilo en cascada para representar adecuadamente el contenido y proporcionar una experiencia fácil de utilizar. La aplicación proporciona un método equivalente para que los usuarios con problemas de visión utilicen los valores de visualización del sistema, incluida la modalidad de contraste alto. Puede controlar el tamaño de fuente utilizando la configuración del dispositivo o del navegador web.

Entre las interfaces web, se incluyen puntos de referencia de navegación WAI-ARIA que se pueden utilizar para ir rápidamente a las áreas funcionales de la aplicación.

Software del proveedor

La familia de productos de IBM Spectrum Protect incluye determinado software de proveedor que no está incluido en el acuerdo de licencia de IBM. IBM no es

responsable de las funciones de accesibilidad de estos productos. Póngase en contacto con el proveedor para ver la información de accesibilidad de sus productos.

Información sobre accesibilidad relacionada

Además del centro de atención al cliente de IBM y los sitios web de soporte, IBM tiene un servicio telefónico TTY que pueden utilizar los clientes sordos o con dificultades auditivas para acceder a los servicios de soporte y ventas:

Servicio TTY
800-IBM-3383 (800-426-3383)
(en Norteamérica)

Para obtener más información sobre el compromiso de IBM con la accesibilidad, consulte el apartado Accesibilidad de IBM (www.ibm.com/able).

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en Estados Unidos. Este material puede estar disponible en IBM en otros idiomas. Sin embargo, es posible que tenga obligación de tener una copia del producto o de la versión del producto en dicho idioma para poder acceder.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante de IBM local para obtener información acerca de los productos y servicios que se encuentran actualmente disponibles en su zona. Cualquier referencia a un producto, programa o servicio de IBM no pretende establecer ni implicar que únicamente se pueda utilizar dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio equivalente que no vulnere los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal descrito en este documento. La posesión de este documento no otorga ninguna licencia sobre dichas patentes. Si lo desea, puede realizar consultas sobre licencias, por escrito, dirigiéndose a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Para realizar consultas sobre licencias relativas a la información del juego de caracteres de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe sus consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, NI EXPRESA NI IMPLÍCITA, INCLUIDAS, PERO NO LIMITADAS A LAS GARANTÍAS IMPLÍCITAS DE NO CUMPLIMIENTO, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunos países no permiten la renuncia de garantías expresas ni implícitas en determinadas transacciones, por lo que esta declaración puede no ser aplicable a su caso.

Esta publicación podría contener imprecisiones técnicas o errores tipográficos. La información que ofrece está sometida a modificaciones periódicas, las cuales se van incorporando en ediciones posteriores de la publicación. IBM puede realizar mejoras o cambios en los productos o programas descritos en esta publicación sin aviso previo.

Cualquier referencia a esta información en sitios web que no son de IBM se proporciona solamente para su comodidad y no equivale de ninguna manera a una aprobación de dichos sitios web. Los materiales de estos sitios web no forman parte de los materiales de este producto de IBM; la utilización de dichos sitios es a cuenta y riesgo del usuario.

IBM podría utilizar o distribuir la información que le envía de la forma que considere más oportuna sin incurrir por ello en ninguna obligación con el remitente de la información.

Los poseedores de licencias de este programa que deseen obtener información sobre éste a efectos de permitir: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deben ponerse en contacto con:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Este tipo de información puede estar disponible, sujeta a los términos y condiciones pertinentes, lo que incluye, en determinados casos, el pago de una cuota.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del Acuerdo del Cliente de IBM, el Acuerdo de Licencia de Programa Internacional de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento que se mencionan aquí se presentan tal como se han obtenido en determinadas condiciones operativas. Los resultados reales pueden variar.

La información acerca de productos ajenos a IBM se ha obtenido de los proveedores de dichos productos, sus anuncios publicados u otras fuentes de disponibilidad pública. IBM no ha probado dichos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni otras afirmaciones relacionadas con productos que no son de IBM. Las preguntas relacionadas con las prestaciones de los productos que no son de IBM deberían dirigirse a los proveedores de dichos productos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones de negocio diarias. Para ilustrarlos, de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos ellos son ficticios y cualquier parecido con nombres y direcciones de empresas reales es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en código fuente, que ilustran técnicas de programación en diferentes plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin incurrir en pago alguno a IBM, para fines de desarrollo, utilización, comercialización o distribución de programas de aplicación destinados a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han

escrito los programas de ejemplo. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por tanto, IBM no puede garantizar ni implicar la fiabilidad, utilidad o función de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL" y sin garantía de ninguna clase. IBM no se responsabiliza de los daños que pudieran derivarse del uso de los programas de ejemplo.

Cada copia o fragmento de estos programas de ejemplo o cualquier trabajo derivado deben incluir un aviso de copyright como el siguiente: © (nombre de su empresa) (año). Partes de este código derivan de programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o años_.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corp., en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de otras empresas. Encontrará una lista actualizada de marcas registradas de IBM en la web, en la sección sobre "Copyright e información sobre marcas registradas" de www.ibm.com/legal/copytrade.shtml.

Adobe es una marca registrada de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Linear Tape-Open, LTO y Ultrium son marcas registradas de HP, IBM Corp. y Quantum en EE.UU. y en otros países.

Intel e Itanium son marcas registradas de Intel Corporation o sus empresas filiales en Estados Unidos y otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y de sus filiales.

SoftLayer es una marca registrada de SoftLayer, Inc., una empresa de IBM.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Términos y condiciones de la documentación del producto

Los permisos para utilizar estas publicaciones se otorgan de acuerdo con los términos y condiciones siguientes.

Validez

Estos términos y condiciones completan los términos y condiciones de uso del sitio web de IBM.

Uso personal

Puede reproducir estas publicaciones para su uso personal, no comercial, siempre y cuando se conserven todos los avisos sobre propiedad. No podrá

distribuir, mostrar, ni crear trabajo derivado de estas publicaciones, o cualquier parte de éstas, sin el consentimiento expreso de IBM.

Uso comercial

Puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de la empresa a condición de que se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de estas publicaciones ni reproducir, distribuir o visualizar estas publicaciones ni parte de las mismas fuera de la empresa sin el consentimiento expreso de IBM.

Derechos

Si no se indica lo contrario en este permiso, no se otorgan otros permisos, licencias o derechos, ya sea de forma expresa o implícita, a las publicaciones u otra información, datos, software u otra propiedad intelectual que contenga este documento.

IBM se reserva el derecho de retirar los permisos aquí concedidos cuando lo desee, siempre que el uso de las publicaciones vaya en detrimento de su interés o, según determine IBM, si no se cumplen correctamente las instrucciones anteriores.

Queda prohibido descargar, exportar o reexportar esta información si no se cumplen íntegramente todas las leyes aplicables y regulaciones, incluyendo las leyes y regulaciones de exportación de los Estados Unidos.

IBM NO GARANTIZA EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPLÍCITAS O IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO INFRACCIÓN Y ADECUACIÓN A UN FIN DETERMINADO.

Consideraciones sobre la política de privacidad

Los productos de IBM Software, incluido el software como soluciones de servicio, (“Ofertas de software”) podrían utilizar cookies u otras tecnologías para recopilar información del uso del producto para ayudar a mejorar la experiencia del usuario final, para adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta oferta de software utiliza cookies para recopilar información de identificación personal, la información específica sobre la utilización de cookies de esta oferta se expone más adelante.

Esta oferta de software no utiliza cookies u otras tecnologías para recopilar información de identificación personal.

Si las configuraciones desplegadas para esta Oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento legal sobre las leyes aplicables a dicha recopilación de datos, incluidos los requisitos de aviso y consentimiento.

Para obtener más información sobre el uso de distintas tecnologías, incluidas las cookies, para estos fines, consulte la Política de privacidad de IBM en http://www.ibm.com/privacy y la Declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details, en la sección “Cookies, Web Beacons and Other Technologies”, e “IBM Software Products and Software-as-a-Service Privacy

Statement" en http://www.ibm.com/software/info/product-privacy.

Glosario

Hay un glosario disponible con términos y definiciones para la familia de productos de IBM Spectrum Protect.

Consulte el apartado Glosario de IBM Spectrum Protect.

Para ver los glosarios de otros productos de IBM, consulte Terminología de IBM.

Índice

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

V

W

Número de Programa: 5725-W98
5725-W99
5725-X15

Impreso en España