



Administre clústeres BeeGFS

BeeGFS on NetApp with E-Series Storage

NetApp
January 27, 2026

Tabla de contenidos

Administre clústeres BeeGFS	1
Descripción general, conceptos clave y terminología	1
Descripción general	1
Conceptos clave	1
Terminología común	2
Cuándo usar Ansible frente a la herramienta pc	2
Examine el estado del clúster	3
Descripción general	3
Comprender el resultado de <code>pcs status</code>	3
Vuelva a configurar el clúster de alta disponibilidad y BeeGFS	4
Descripción general	4
Cómo deshabilitar y activar delimitación	5
Actualice los componentes de clúster de alta disponibilidad	5
Actualizar los servicios BeeGFS	5
Actualiza a BeeGFS v8	9
Actualice los paquetes Pacemaker y Corosync en un clúster HA	19
Actualice el firmware del adaptador de nodo de archivo	22
Actualice la cabina de almacenamiento E-Series	26
Mantenimiento y mantenimiento	28
Servicios de conmutación por error y conmutación tras recuperación	28
Coloque el clúster en modo de mantenimiento	31
Detenga e inicie el clúster	32
Sustituya los nodos de archivo	33
Expanda o reduzca el clúster	34
Solucionar problemas	36
Descripción general	36
Guías de solución de problemas	36
Cuestiones comunes	40
Tareas comunes de solución de problemas	41

Administre clústeres BeeGFS

Descripción general, conceptos clave y terminología

Obtenga información sobre cómo administrar los clústeres de alta disponibilidad de BeeGFS después de haberse puesto en marcha.

Descripción general

Esta sección está destinada a administradores de clústeres que deben gestionar clústeres de alta disponibilidad de BeeGFS una vez que se han puesto en marcha. Incluso los que estén familiarizados con los clústeres de alta disponibilidad de Linux deben leer esta guía detenidamente, ya que hay varias diferencias en cómo gestionar el clúster, especialmente en lo que respecta a la reconfiguración debido al uso de Ansible.

Conceptos clave

Aunque algunos de estos conceptos se introducen en "["términos y conceptos"](#)" la página principal, es útil reintroducirlos en el contexto de un clúster de alta disponibilidad de BeeGFS:

Nodo de clúster: servidor que ejecuta los servicios Pacemaker y Corosync y que participa en el clúster ha.

Nodo de archivo: un nodo de clúster utilizado para ejecutar uno o más servicios de gestión, metadatos o almacenamiento de BeeGFS.

Nodo de bloque: Un sistema de almacenamiento E-Series de NetApp que proporciona almacenamiento basado en bloques a los nodos de ficheros. Estos nodos no participan en el clúster de alta disponibilidad de BeeGFS porque proporcionan sus propias funcionalidades de alta disponibilidad independientes. Cada nodo consta de dos controladoras de almacenamiento que proporcionan alta disponibilidad en la capa de bloques.

Servicio BeeGFS: un servicio de gestión, metadatos o almacenamiento de BeeGFS. Cada nodo de archivo ejecutará uno o más servicios que usarán volúmenes en el nodo de bloque para almacenar sus datos.

Elementos básicos: una puesta en marcha estandarizada de nodos de archivos BeeGFS, nodos de bloque E-Series y servicios BeeGFS que se ejecutan en ellos simplifican el escalado de un clúster/sistema de archivos de alta disponibilidad de BeeGFS siguiendo una arquitectura verificada de NetApp. También se admiten clústeres de alta disponibilidad personalizados, pero a menudo siguen un método de elementos básicos similar para simplificar el escalado.

BeeGFS ha Cluster: un número escalable de nodos de archivo utilizados para ejecutar servicios BeeGFS respaldados por nodos de bloque para almacenar los datos de BeeGFS de forma muy disponible. Desarrollado a partir de componentes de código abierto demostrados en el sector Pacemaker y Corosync con Ansible para el paquete y la puesta en marcha.

Servicios de Cluster Server: se refiere a los servicios Pacemaker y Corosync que se ejecutan en cada nodo que participa en el cluster. Tenga en cuenta que es posible que un nodo no ejecute ningún servicio BeeGFS y solo participe en el clúster como nodo "tiebreaker" en el caso de que solo haya necesidad de dos nodos de archivo.

Recursos de clúster: para cada servicio BeeGFS que se ejecuta en el clúster, verá un recurso de supervisión BeeGFS y un grupo de recursos que contiene recursos para los objetivos BeeGFS, direcciones IP (IP flotantes) y el servicio BeeGFS mismo.

Ansible: una herramienta para el aprovisionamiento de software, la gestión de la configuración y la puesta en

marcha de aplicaciones, lo que permite la infraestructura como código. Así es como los clústeres de alta disponibilidad de BeeGFS se empaquetan para simplificar el proceso de puesta en marcha, reconfiguración y actualización de BeeGFS en NetApp.

pc: una interfaz de línea de comandos disponible desde cualquiera de los nodos de archivos del clúster utilizados para consultar y controlar el estado de los nodos y recursos del clúster.

Terminología común

Failover: cada servicio BeeGFS tiene un nodo de archivo preferido en el que se ejecutará a menos que dicho nodo falle. Cuando un servicio BeeGFS se ejecuta en un nodo de archivo no preferido/secundario, se dice que está en comutación por error.

Fallback: el acto de mover servicios BeeGFS de un nodo de archivo no preferido de nuevo a su nodo preferido.

Par de alta disponibilidad: dos nodos de archivo que pueden acceder al mismo conjunto de nodos de bloque se denominan a veces pares de alta disponibilidad. Este es un término común que se emplea en NetApp para hacer referencia a dos controladoras de almacenamiento o nodos que se pueden «sustituir» entre sí.

Modo de mantenimiento: desactiva la supervisión de todos los recursos e impide que Pacemaker mueva o administre de otro modo los recursos en el clúster (consulte también la sección en "[modo de mantenimiento](#)").

Clúster de alta disponibilidad: uno o más nodos de archivo que ejecutan servicios BeeGFS que pueden comutar por error entre varios nodos del clúster para crear un sistema de archivos BeeGFS de alta disponibilidad. A menudo, los nodos de archivo se configuran en pares de alta disponibilidad que pueden ejecutar un subconjunto de los servicios de BeeGFS del clúster.

Cuándo usar Ansible frente a la herramienta pc

¿Cuándo debe utilizar Ansible frente a la herramienta de línea de comandos de pc para gestionar el clúster de alta disponibilidad?

Todas las tareas de puesta en marcha y reconfiguración del clúster se deben completar con Ansible desde un nodo de control externo de Ansible. Normalmente, los cambios temporales en el estado del clúster (por ejemplo, la colocación de nodos dentro y fuera de espera) se realizarán iniciando sesión en un nodo del clúster (preferiblemente uno que no esté degradado o esté a punto de someterse a tareas de mantenimiento) y utilizando la herramienta de línea de comandos del pc.

La modificación de cualquier configuración del clúster, incluidos los recursos, las restricciones, las propiedades y los propios servicios de BeeGFS, siempre debe realizarse con Ansible. Mantener una copia actualizada del inventario y el libro de estrategia de Ansible (lo ideal para un control de origen para realizar un seguimiento de los cambios) forma parte del mantenimiento del clúster. Si necesita realizar cambios en la configuración, actualice el inventario y vuelva a ejecutar el libro de aplicaciones de Ansible que importa el rol de alta disponibilidad de BeeGFS.

El rol de alta disponibilidad manejará colocar el clúster en modo de mantenimiento y, a continuación, hará los cambios necesarios antes de reiniciar BeeGFS o los servicios de clúster para aplicar la nueva configuración. Dado que normalmente no es necesario reiniciar el nodo completo fuera de la puesta en marcha inicial, Ansible se considera un procedimiento "seguro", pero siempre es un procedimiento recomendado durante las ventanas de mantenimiento o fuera de las horas, en caso de que se deban reiniciar los servicios de BeeGFS. Normalmente, estos reinicios no deben causar errores en la aplicación, pero pueden afectar al rendimiento (que algunas aplicaciones pueden manejar mejor que otras).

La repetición de la operación de Ansible también es una opción cuando desea devolver todo el clúster a un estado completamente óptimo y, en algunos casos, puede recuperar el estado del clúster con más facilidad que con los pc. Especialmente durante una emergencia en la que el clúster está inactivo por algún motivo, una vez que todos los nodos se vuelven a ejecutar Ansible puede recuperar el clúster de forma más rápida y fiable que intentar usar los pc.

Examine el estado del clúster

Utilice pc para ver el estado del clúster.

Descripción general

Ejecutando `pcs status` Desde cualquiera de los nodos del clúster es la forma más sencilla de ver el estado general del clúster y el estado de cada recurso (como los servicios BeeGFS y sus dependencias). En esta sección se describe lo que encontrará en el resultado del `pcs status` comando.

Comprender el resultado de `pcs status`

Ejecución `pcs status` En cualquier nodo de clúster en el que se hayan iniciado los servicios de clúster (Pacemaker y Corosync). La parte superior del resultado le mostrará un resumen del clúster:

```
[root@beegfs_01 ~]# pcs status
Cluster name: hacluster
Cluster Summary:
  * Stack: corosync
  * Current DC: beegfs_01 (version 2.0.5-9.el8_4.3-ba59be7122) - partition
with quorum
    * Last updated: Fri Jul  1 13:37:18 2022
    * Last change:  Fri Jul  1 13:23:34 2022 by root via cibadmin on
beegfs_01
    * 6 nodes configured
    * 235 resource instances configured
```

En la siguiente sección se enumeran los nodos del clúster:

```
Node List:
  * Node beegfs_06: standby
  * Online: [ beegfs_01 beegfs_02 beegfs_04 beegfs_05 ]
  * OFFLINE: [ beegfs_03 ]
```

Esto indica notablemente cualquier nodo que esté en espera o sin conexión. Los nodos en espera siguen participando en el clúster, pero se marcan como no aptos para ejecutar los recursos. Los nodos que están sin conexión indican que los servicios de clúster no se están ejecutando en ese nodo, ya sea debido a que se detuvo manualmente o porque el nodo se reinició/apague.



Cuando se inician por primera vez los nodos, se detienen los servicios del clúster y se deben iniciar manualmente para evitar que se reproduzcan accidentalmente los recursos de un nodo que no está en buen estado.

Si los nodos están en espera o sin conexión debido a un motivo no administrativo (por ejemplo, un fallo), se mostrará texto adicional junto al estado del nodo entre paréntesis. Por ejemplo, si está desactivada la delimitación y un recurso encuentra un error que verá Node <HOSTNAME>: standby (on-fail). Otro estado posible es Node <HOSTNAME>: UNCLEAN (offline), que se verá brevemente como un nodo está siendo vallado, pero persistirá si falló la cercado indicando que el clúster no puede confirmar el estado del nodo (esto puede bloquear que los recursos comiencen en otros nodos).

En la siguiente sección se muestra una lista de todos los recursos del clúster y sus estados:

Full List of Resources:

```
* mgmt-monitor    (ocf::eseries:beegfs-monitor):     Started beegfs_01
* Resource Group: mgmt-group:
  * mgmt-FS1     (ocf::eseries:beegfs-target):      Started beegfs_01
  * mgmt-IP1     (ocf::eseries:beegfs-ipaddr2):     Started beegfs_01
  * mgmt-IP2     (ocf::eseries:beegfs-ipaddr2):     Started beegfs_01
  * mgmt-service  (systemd:beegfs-mgtd):           Started beegfs_01
[...]
```

De forma similar a los nodos, se mostrará texto adicional junto al estado del recurso entre paréntesis si hay problemas con el recurso. Por ejemplo, si Pacemaker solicita una detención de recursos y no puede completarse dentro del tiempo asignado, Pacemaker intentará cercar el nodo. Si se desactiva la delimitación o se produce un error en la operación de delimitación, el estado del recurso será FAILED <HOSTNAME> (blocked) Y Pacemaker no podrá iniciarla en un nodo diferente.

Vale la pena destacar que los clusters de ha de BeeGFS utilizan una serie de agentes de recursos de OCF personalizados optimizados de BeeGFS. En particular, el monitor BeeGFS es responsable de activar una conmutación por error cuando los recursos de BeeGFS en un nodo determinado no están disponibles.

Vuelva a configurar el clúster de alta disponibilidad y BeeGFS

Use Ansible para volver a configurar el clúster.

Descripción general

Normalmente, la reconfiguración de cualquier aspecto del clúster de alta disponibilidad de BeeGFS se debe realizar actualizando `ansible-playbook` el inventario de Ansible y volviendo a ejecutar el comando. Esto incluye la actualización de alertas, el cambio de la configuración permanente de la vallado o el ajuste de la configuración del servicio BeeGFS. Estos se ajustan utilizando el `group_vars/ha_cluster.yml` archivo y se puede encontrar una lista completa de opciones en la "[Especifique la configuración de nodos de archivos comunes](#)" sección.

Consulte a continuación para obtener más información sobre opciones de configuración seleccionadas que los administradores deben conocer al realizar tareas de mantenimiento o mantenimiento del clúster.

Cómo deshabilitar y activar delimitación

La cercado se habilita o requiere de forma predeterminada cuando se configura el clúster. En algunos casos, puede que sea conveniente desactivar temporalmente la delimitación para garantizar que los nodos no se cierren accidentalmente al realizar determinadas operaciones de mantenimiento (como la actualización del sistema operativo). Aunque esto se puede desactivar manualmente, hay sacrificios que los administradores deben tener en cuenta.

OPCIÓN 1: Desactive la esgrima con Ansible (recomendado).

Cuando se desactiva el cercado mediante Ansible, la acción en caso de fallo del monitor BeeGFS cambia de "cerca" a "en espera". Esto significa que si el monitor BeeGFS detecta un fallo, intentará poner el nodo en espera y realizar una comutación por error de todos los servicios de BeeGFS. Fuera de la solución activa de problemas/pruebas esto es normalmente más deseable que la opción 2. La desventaja es que si un recurso no se detiene en el nodo original, se impedirá que se inicie en otro lugar (por lo que normalmente se requiere cercado para los clústeres de producción).

1. En su inventario de Ansible en `groups_vars/ha_cluster.yml` añada la siguiente configuración:

```
beegfs_ha_cluster_crm_config_options:  
  stonith-enabled: False
```

2. Vuelva a ejecutar el libro de estrategia de Ansible para aplicar los cambios al clúster.

OPCIÓN 2: Desactive la delimitación manualmente.

En algunos casos puede que desee deshabilitar temporalmente la delimitación sin volver a leer Ansible, quizás para facilitar la solución de problemas o las pruebas del clúster.

 En esta configuración si el monitor BeeGFS detecta un error, el clúster intentará detener el grupo de recursos correspondiente. NO activará una comutación por error completa ni intentará reiniciar ni mover el grupo de recursos afectado a otro host. Para recuperarse, solucione cualquier problema que se pueda ejecutar `pcs resource cleanup` o coloque manualmente el nodo en espera.

Pasos:

1. Para determinar si el cercado (stonith) está habilitado o desactivado globalmente, ejecute: `pcs property show stonith-enabled`
2. Para desactivar la secuencia de cercado: `pcs property set stonith-enabled=false`
3. Para habilitar la ejecución de cercado: `pcs property set stonith-enabled=true`

 Esta configuración se anulará la próxima vez que ejecute el playbook de Ansible.

Actualice los componentes de clúster de alta disponibilidad

Actualizar los servicios BeeGFS

Usa Ansible para actualizar la versión de BeeGFS que se ejecuta en tu clúster de HA.

Descripción general

BeeGFS sigue un `major.minor.patch` esquema de control de versiones. Se proporcionan los roles de Ansible de alta disponibilidad de BeeGFS para cada `major.minor` versión compatible (p. ej., `beegfs_ha_7_2` y `beegfs_ha_7_3`). Todos los roles de alta disponibilidad se fijan a la última versión de parche de BeeGFS disponible en el momento del lanzamiento de la colección Ansible.

Ansible se debe usar para todas las actualizaciones de BeeGFS, incluyendo el cambio entre versiones principales, menores y de parches de BeeGFS. Para actualizar BeeGFS primero necesitas actualizar la colección BeeGFS Ansible, lo que también traerá las últimas correcciones y mejoras en la automatización de despliegue/gestión y el clúster HA subyacente. Incluso después de actualizar a la última versión de la colección, BeeGFS no se actualizará hasta que se ejecute `ansible-playbook` con la opción `-e "beegfs_ha_force_upgrade=true"` activada. Para más detalles sobre cada actualización, consulta la ["Documentación de actualización de BeeGFS"](#) para tu versión actual.



Si estás actualizando a BeeGFS v8, consulta el procedimiento ["Actualiza a BeeGFS v8"](#) en su lugar.

Rutas de actualización probadas

Se han probado y verificado las siguientes rutas de actualización:

Versión original	Actualizar la versión	MultiRail	Detalles
7.2.6	7.3.2	Sí	Actualización de la colección beegfs de v3.0.1 a v3.1.0, multirail agregó
7.2.6	7.2.8	No	Actualizando la colección beegfs de v3.0.1 a v3.1.0
7.2.8	7.3.1	Sí	Actualización mediante la colección beegfs v3.1.0, multirail añadido
7.3.1	7.3.2	Sí	Actualice utilizando beegfs Collection v3.1.0
7.3.2	7.4.1	Sí	Actualice utilizando beegfs Collection v3.2.0
7.4.1	7.4.2	Sí	Actualice utilizando beegfs Collection v3.2.0
7.4.2	7.4.6	Sí	Actualice utilizando beegfs Collection v3.2.0
7.4.6	8,0	Sí	Actualiza usando las instrucciones en el procedimiento "Actualiza a BeeGFS v8" .
7.4.6	8,1	Sí	Actualiza usando las instrucciones en el procedimiento "Actualiza a BeeGFS v8" .
7.4.6	8,2	Sí	Actualiza usando las instrucciones en el procedimiento "Actualiza a BeeGFS v8" .

Pasos de actualización de BeeGFS

En las siguientes secciones se ofrecen pasos para actualizar la colección Ansible BeeGFS y el propio BeeGFS. Preste especial atención a cualquier paso(s) adicional(s) para actualizar BeeGFS versiones mayores o menores.

Paso 1: Actualizar la colección BeeGFS

Para actualizaciones de colecciones con acceso a "Galaxia de ansible", ejecute el siguiente comando:

```
ansible-galaxy collection install netapp_eseries.beegfs --upgrade
```

Para actualizaciones de colecciones sin conexión, descargue la colección desde "Galaxia de ansible" haciendo clic en el deseado Install Version` y después Download tarball. Transfiera el tarball al nodo de control de Ansible y ejecute el siguiente comando.

```
ansible-galaxy collection install netapp_eseries-beegfs-<VERSION>.tar.gz  
--upgrade
```

Consulte "[Instalando colecciones](#)" si quiere más información.

Paso 2: Actualice el inventario de Ansible

Haz cualquier actualización necesaria o que quieras en los archivos de inventario de Ansible de tu clúster. Mira la sección [Notas de actualización de la versión](#) abajo para ver detalles sobre tus requisitos específicos de actualización. Mira la sección "[Descripción general del inventario de Ansible](#)" para información general sobre cómo configurar tu inventario de BeeGFS HA.

Paso 3: Actualizar Ansible playbook (cuando se actualizan solo versiones principales o secundarias)

Si va a cambiar entre versiones principal o secundaria, en `playbook.yml` el archivo usado para implementar y mantener el clúster, actualice el nombre `beegfs_ha_<VERSION>` del rol para reflejar la versión deseada. Por ejemplo, si desea desplegar BeeGFS 7.4, esto sería `beegfs_ha_7_4`:

```
- hosts: all
gather_facts: false
any_errors_fatal: true
collections:
  - netapp_eseries.beegfs
tasks:
  - name: Ensure BeeGFS HA cluster is setup.
    ansible.builtin.import_role: # import_role is required for tag availability.
    name: beegfs_ha_7_4
```

Si desea obtener más información sobre el contenido de este archivo de playbook, consulte "[Ponga en marcha el clúster de alta disponibilidad de BeeGFS](#)" la sección.

Paso 4: Ejecute la actualización de BeeGFS

Para aplicar la actualización de BeeGFS:

```
ansible-playbook -i inventory.yml beegfs_ha_playbook.yml -e  
"beegfs_ha_force_upgrade=true" --tags beegfs_ha
```

Entre bastidores, el rol de BeeGFS ha se encargará de:

- Asegúrese de que el clúster esté en estado óptimo en cada servicio BeeGFS ubicado en su nodo preferido.
- Ponga el clúster en modo de mantenimiento.
- Actualice los componentes del clúster de alta disponibilidad (si es necesario).
- Actualice cada nodo de archivo de uno en uno de los siguientes modos:
 - Colóquela en espera y realice la conmutación al nodo de respaldo de sus servicios en el nodo secundario.
 - Actualizar paquetes BeeGFS.
 - Servicios de respaldo.
- Mueva el clúster fuera del modo de mantenimiento.

Notas de actualización de la versión

Actualización desde BeeGFS versión 7.2.6 o 7.3.0

Cambios en la autenticación basada en conexión

BeeGFS versión 7.3.2 y posteriores requieren que se configure la autenticación basada en conexión. Los servicios no se iniciarán sin una de las siguientes opciones:

- Especificar un connAuthFile, o
- Configuración connDisableAuthentication=true en el archivo de configuración del servicio.

Se recomienda encarecidamente activar la autenticación basada en conexión por seguridad. Consulta "[Autenticación basada en conexión BeeGFS](#)" para más información.

Los beegfs_ha* roles generan y distribuyen automáticamente el archivo de autenticación a:

- Todos los nodos de archivos en el clúster
- El nodo de control de Ansible en
`<playbook_directory>/files/beegfs/<beegfs_mgmt_ip_address>_connAuthFile`

La beegfs_client función detectará y aplicará automáticamente este archivo a los clientes cuando esté presente.

 Si no usaste el rol beegfs_client para configurar clientes, debes distribuir manualmente el archivo de autenticación a cada cliente y configurar la opción connAuthFile en el archivo beegfs-client.conf. Al actualizar desde una versión de BeeGFS sin autenticación basada en conexión, los clientes perderán el acceso a menos que desactives la autenticación basada en conexión durante la actualización configurando beegfs_ha_conn_auth_enabled: false en group_vars/ha_cluster.yml (no recomendado).

Para más detalles y opciones de configuración alternativas, consulta el paso de configuración de autenticación de la conexión en la sección "[Especifique la configuración de nodos de archivos comunes](#)".

Actualiza a BeeGFS v8

Sigue estos pasos para actualizar tu clúster BeeGFS HA de la versión 7.4.6 a BeeGFS v8.

Descripción general

BeeGFS v8 introduce varios cambios significativos que requieren una configuración adicional antes de actualizar desde BeeGFS v7. Este documento te guía para preparar tu clúster para los nuevos requisitos de BeeGFS v8 y luego actualizar a BeeGFS v8.

 Antes de actualizar a BeeGFS v8, asegúrate de que tu sistema está ejecutando al menos BeeGFS 7.4.6. Cualquier clúster que esté ejecutando una versión anterior a BeeGFS 7.4.6 debe primero "[actualiza a la versión 7.4.6](#)" antes de continuar con este procedimiento de actualización a BeeGFS v8.

Cambios clave en BeeGFS v8

BeeGFS v8 introduce los siguientes cambios importantes:

- **Cumplimiento de licencias:** BeeGFS v8 requiere una licencia para usar funciones premium como grupos de almacenamiento, objetivos de almacenamiento remotos, BeeOND y más. Adquiere una licencia válida para tu clúster BeeGFS antes de actualizar. Si lo necesitas, puedes obtener una licencia de evaluación temporal de BeeGFS v8 desde el "[Portal de Licencias de BeeGFS](#)".
- **Migración de bases de datos del servicio de gestión:** Para habilitar la configuración con el nuevo formato basado en TOML en BeeGFS v8, tienes que migrar manualmente tu base de datos del servicio de gestión de BeeGFS v7 al formato actualizado de BeeGFS v8.
- **Encriptación TLS:** BeeGFS v8 introduce TLS para una comunicación segura entre servicios. Tendrás que generar y distribuir certificados TLS para el servicio de gestión de BeeGFS y la utilidad de línea de comandos `beegfs` como parte de la actualización.

Para más detalles y cambios adicionales en BeeGFS 8, consulta la "[Guía de actualización de BeeGFS v8.0.0](#)".

 La actualización a BeeGFS v8 requiere tiempo de inactividad del clúster. Además, los clientes BeeGFS v7 no pueden conectarse a los clústeres BeeGFS v8. Coordina cuidadosamente el momento de la actualización entre el clúster y los clientes para minimizar el impacto en las operaciones.

Prepara tu clúster BeeGFS para la actualización

Antes de iniciar la actualización, prepara cuidadosamente tu entorno para asegurar una transición fluida y minimizar el tiempo de inactividad.

1. Asegúrate de que tu clúster esté en buen estado y que todos los servicios BeeGFS se estén ejecutando en sus nodos preferidos. Desde un nodo de archivos que ejecuta servicios BeeGFS, verifica que todos los recursos Pacemaker se estén ejecutando en sus nodos preferidos:

```
pcs status
```

2. Registra y haz una copia de seguridad de la configuración de tu clúster.
 - a. Consulta "[Documentación de copia de seguridad de BeeGFS](#)" para obtener instrucciones sobre cómo hacer una copia de seguridad de la configuración del clúster.
 - b. Haz una copia de seguridad del directorio de datos de gestión existente:

```
cp -r /mnt/mgmt_tgt_mgmt01/data  
/mnt/mgmt_tgt_mgmt01/data_beegfs_v7_backup_$(date +%Y%m%d)
```

- c. Ejecuta los siguientes comandos desde un cliente beegfs y guarda su salida como referencia:

```
beegfs-ctl --getentryinfo --verbose /path/to/beegfs/mountpoint
```

- d. Si usas la duplicación, recopila información de estado detallada:

```
beegfs-ctl --listtargets --longnodes --state --spaceinfo  
--mirrorgroups --nodetype=meta  
beegfs-ctl --listtargets --longnodes --state --spaceinfo  
--mirrorgroups --nodetype=storage
```

3. Prepara a tus clientes para el tiempo de inactividad y detén los servicios beegfs-client. Para cada cliente, ejecuta:

```
systemctl stop beegfs-client
```

4. Para cada clúster Pacemaker, desactiva STONITH. Esto te permitirá validar la integridad del clúster después de la actualización sin provocar reinicios innecesarios de nodos.

```
pcs property set stonith-enabled=false
```

5. Para todos los clústeres Pacemaker en el espacio de nombres BeeGFS, usa PCS para detener el clúster:

```
pcs cluster stop --all
```

Actualiza los paquetes BeeGFS

En todos los nodos de archivos del clúster, agrega el repositorio de paquetes BeeGFS v8 para tu distribución de Linux. Las instrucciones para usar los repositorios oficiales de BeeGFS se pueden encontrar en "["Página de descarga de BeeGFS"](#)". De lo contrario, configura tu repositorio local de réplica de beegfs según corresponda.

Los siguientes pasos muestran cómo usar el repositorio oficial BeeGFS 8.2 en los nodos de archivos RHEL 9. Realiza los siguientes pasos en todos los nodos de archivos del clúster:

1. Importa la clave GPG de BeeGFS:

```
rpm --import https://www.beegfs.io/release/beegfs_8.2/gpg/GPG-KEY-beegfs
```

2. Importa el repositorio BeeGFS:

```
curl -L -o /etc/yum.repos.d/beegfs-rhel9.repo  
https://www.beegfs.io/release/beegfs_8.2/dists/beegfs-rhel9.repo
```



Elimina cualquier repositorio BeeGFS previamente configurado para evitar conflictos con el nuevo repositorio BeeGFS v8.

3. Limpia la caché de tu gestor de paquetes:

```
dnf clean all
```

4. En todos los nodos de archivos, actualiza los paquetes BeeGFS a BeeGFS 8.2.

```
dnf update beegfs-mgtd beegfs-storage beegfs-meta libbeegfs-ib
```



En un clúster estándar, el paquete `beegfs-mgtd` solo se actualizará en los dos primeros nodos de archivos.

Actualiza la base de datos de gestión

En uno de los nodos de archivos que ejecutan el servicio de gestión BeeGFS, realiza los siguientes pasos para migrar la base de datos de gestión de BeeGFS v7 a v8.

1. Enumera todos los dispositivos NVMe y filtra el destino de gestión:

```
nvme netapp smdevices | grep mgmt_tgt
```

- Toma nota de la ruta del dispositivo de la salida.
- Monta el dispositivo de destino de gestión en el punto de montaje de destino de gestión existente (reemplaza `/dev/nvmeXnY` por la ruta de tu dispositivo):

```
mount /dev/nvmeXnY /mnt/mgmt_tgt_mgmt01/
```

2. Importa tus datos de gestión de BeeGFS 7 al nuevo formato de base de datos ejecutando:

```
/opt/beegfs/sbin/beegfs-mgmtd --import-from  
-v7=/mnt/mgmt_tgt_mgmt01/data/
```

Salida esperada:

```
Created new database version 3 at "/var/lib/beegfs/mgmtd.sqlite".  
Successfully imported v7 management data from  
"/mnt/mgmt_tgt_mgmt01/data/".
```



Es posible que la importación automática no se realice correctamente en todos los casos debido a los requisitos de validación más estrictos en BeeGFS v8. Por ejemplo, si los objetivos se asignan a grupos de almacenamiento que no existen, la importación fallará. Si la migración falla, no sigas con la actualización. Contacta al soporte de NetApp para que te ayuden a resolver los problemas de migración de bases de datos. Como solución provisional, puedes bajar la versión de los paquetes de BeeGFS v8 y seguir usando BeeGFS v7 mientras se resuelve el problema.

3. Mueve el archivo SQLite generado al montaje del servicio de gestión:

```
mv /var/lib/beegfs/mgmtd.sqlite /mnt/mgmt_tgt_mgmt01/data/
```

4. Mueve el `beegfs-mgmtd.toml` generado al montaje del servicio de gestión:

```
mv /etc/beegfs/beegfs-mgmtd.toml /mnt/mgmt_tgt_mgmt01/mgmt_config/
```

Preparar el archivo de configuración `beegfs-mgmtd.toml` se hará después de completar los pasos de licenciamiento y configuración de TLS en las próximas secciones.

Configura licencias

1. Instala los paquetes de licencia beegfs en todos los nodos que ejecutan el servicio de gestión beegfs. Esto suele ser en los dos primeros nodos del clúster:

```
dnf install libbeegfs-license
```

2. Descarga tu archivo de licencia de BeeGFS v8 en los nodos de gestión y colócalo en:

```
/etc/beegfs/license.pem
```

Configura el cifrado TLS

BeeGFS v8 requiere el cifrado TLS para una comunicación segura entre los servicios de gestión y los clientes. Hay tres opciones para configurar el cifrado TLS en las comunicaciones de red entre los servicios de gestión y los servicios cliente. El método recomendado y más seguro es usar certificados firmados por una Certificate Authority de confianza. Como alternativa, puedes crear tu propia CA local para firmar certificados para tu clúster BeeGFS. Para entornos donde el cifrado no es necesario o para solucionar problemas, TLS se puede deshabilitar por completo, aunque esto no se recomienda porque expone información sensible a la red.

Antes de continuar, sigue las instrucciones de la guía "["Configura el cifrado TLS para BeeGFS 8"](#)" para configurar el cifrado TLS en tu entorno.

Actualizar la configuración del servicio de gestión

Prepara el archivo de configuración del servicio de gestión de BeeGFS v8 transfiriendo manualmente los ajustes de tu archivo de configuración de BeeGFS v7 en el archivo /mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml.

1. En el nodo de gestión con el objetivo de gestión montado, consulta el archivo de servicio de gestión /mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.conf para BeeGFS 7 y luego transfiere todos los ajustes al archivo /mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml. Para una configuración básica, tu beegfs-mgmtd.toml puede verse así:

```
beemsg-port = 8008
grpc-port = 8010
log-level = "info"
node-offline-timeout = "900s"
quota-enable = false
auth-disable = false
auth-file = "/etc/beegfs/<mgmt_service_ip>_connAuthFile"
db-file = "/mnt/mgmt_tgt_mgmt01/data/mgmtd.sqlite"
license-disable = false
license-cert-file = "/etc/beegfs/license.pem"
tls-disable = false
tls-cert-file = "/etc/beegfs/mgmtd_tls_cert.pem"
tls-key-file = "/etc/beegfs/mgmtd_tls_key.pem"
interfaces = ['i1b:mgmt_1', 'i2b:mgmt_2']
```

Ajusta todas las rutas según sea necesario para que coincidan con tu entorno y configuración TLS.

2. En cada nodo de archivo que ejecuta servicios de gestión, modifica tu archivo de servicio systemd para que apunte a la nueva ubicación del archivo de configuración.

```
sudo sed -i 's|ExecStart=.*|ExecStart=nice -n -3
/opt/beegfs/sbin/beegfs-mgmtd --config-file
/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml|'
/etc/systemd/system/beegfs-mgmtd.service
```

- a. Recarga systemd:

```
systemctl daemon-reload
```

3. Para cada nodo de archivos que ejecuta servicios de gestión, abre el puerto 8010 para la comunicación gRPC del servicio de gestión.

- a. Agrega el puerto 8010/tcp a la zona beegfs:

```
sudo firewall-cmd --zone=beegfs --permanent --add-port=8010/tcp
```

- b. Recarga el cortafuegos para aplicar el cambio:

```
sudo firewall-cmd --reload
```

Actualiza el script de monitor de BeeGFS

El script OCF de Pacemaker `beegfs-monitor` requiere actualizaciones para ser compatible con el nuevo formato de configuración TOML y la gestión de servicios systemd. Actualiza el script en un nodo del clúster y luego copia el script actualizado a todos los demás nodos.

1. Crea una copia de seguridad del script actual:

```
cp /usr/lib/ocf/resource.d/eseries/beegfs-monitor  
/usr/lib/ocf/resource.d/eseries/beegfs-monitor.bak.$(date +%F)
```

2. Actualiza la ruta del archivo de configuración de `.conf` a `.toml`:

```
sed -i 's|mgmt_config/beegfs-mgtd\.conf|mgmt_config/beegfs-mgtd.toml|'  
/usr/lib/ocf/resource.d/eseries/beegfs-monitor
```

Alternativamente, localiza manualmente el siguiente bloque en el script:

```
case $type in  
management)  
    conf_path="${configuration_mount}/mgmt_config/beegfs-mgtd.conf"  
;;
```

Y reemplázalo por:

```
case $type in
management)
    conf_path="${configuration_mount}/mgmt_config/beegfs-mgmtd.toml"
;;

```

3. Actualiza las funciones `get_interfaces()` y `get_subnet_ips()` para admitir la configuración de TOML:

- a. Abre el script en un editor de texto:

```
vi /usr/lib/ocf/resource.d/eseries/beegfs-monitor
```

- b. Localiza las dos funciones: `get_interfaces()` y `get_subnet_ips()`.
- c. Elimina ambas funciones completas, empezando en `get_interfaces()` hasta el final de `get_subnet_ips()`.
- d. Copia y pega las siguientes funciones actualizadas en su lugar:

```

# Return network communication interface name(s) from the BeeGFS
resource's connInterfaceFile
get_interfaces() {
    # Determine BeeGFS service network IP interfaces.
    if [ "$type" = "management" ]; then
        interfaces_line=$(grep "^interfaces =" "$conf_path")
        interfaces_list=$(echo "$interfaces_line" | sed "s/.*= \[\(\.\*
        \)\]\/\(\d\)/")
        interfaces=$(echo "$interfaces_list" | tr -d '"' | tr -d " " | tr
        ',' '\n')

        for entry in $interfaces; do
            echo "$entry" | cut -d ':' -f 1
        done
    else
        connInterfacesFile_path=$(grep "^connInterfacesFile" "$conf_path"
        | tr -d "[[:space:]]" | cut -f 2 -d "=")

        if [ -f "$connInterfacesFile_path" ]; then
            while read -r entry; do
                echo "$entry" | cut -f 1 -d ':'
            done < "$connInterfacesFile_path"
        fi
    fi
}

# Return list containing all the BeeGFS resource's usable IP
addresses. *Note that these are filtered by the connNetFilterFile
entries.
get_subnet_ips() {
    # Determine all possible BeeGFS service network IP addresses.
    if [ "$type" != "management" ]; then
        connNetFilterFile_path=$(grep "^connNetFilterFile" "$conf_path" |
        tr -d "[[:space:]]" | cut -f 2 -d "=")

        filter_ips=""
        if [ -n "$connNetFilterFile_path" ] && [ -e
$connNetFilterFile_path ]; then
            while read -r filter; do
                filter_ips="$filter_ips $(get_ipv4_subnet_addresses $filter)"
            done < $connNetFilterFile_path
        fi

        echo "$filter_ips"
    fi
}

```

- e. Guarda y sal del editor de texto.
- f. Ejecuta el siguiente comando para comprobar si el script tiene errores de sintaxis antes de continuar.
Si no hay salida, significa que el script es sintácticamente correcto.

```
bash -n /usr/lib/ocf/resource.d/eseries/beegfs-monitor
```

4. Copia el script `beegfs-monitor` OCF actualizado en todos los demás nodos del clúster para asegurar la coherencia:

```
scp /usr/lib/ocf/resource.d/eseries/beegfs-monitor  
user@node:/usr/lib/ocf/resource.d/eseries/beegfs-monitor
```

Vuelve a poner en línea el clúster

1. Una vez completados todos los pasos de actualización anteriores, pon el clúster en línea iniciando los servicios BeeGFS en todos los nodos.

```
pcs cluster start --all
```

2. Verifica que el servicio `beegfs-mgtd` se inició correctamente:

```
journalctl -xeu beegfs-mgtd
```

La salida esperada incluye líneas como:

```
Started Cluster Controlled beegfs-mgtd.  
Loaded config file from "/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-  
mgtd.toml"  
Successfully initialized certificate verification library.  
Successfully loaded license certificate: TMP-113489268  
Opened database at "/mnt/mgmt_tgt_mgmt01/data/mgtd.sqlite"  
Listening for BeeGFS connections on [::]:8008  
Serving gRPC requests on [::]:8010
```



Si aparecen errores en los registros del diario, revisa las rutas del archivo de configuración de gestión y asegúrate de que todos los valores se hayan transferido correctamente desde el archivo de configuración de BeeGFS 7.

3. Ejecuta `pcs status` y verifica que el clúster está saludable y que los servicios se inician en sus nodos preferidos.
4. Una vez que se verifica que el clúster está saludable, vuelve a habilitar STONITH:

```
pcs property set stonith-enabled=true
```

5. Ve a la siguiente sección para actualizar los clientes BeeGFS en el clúster y revisar la salud del clúster BeeGFS.

Actualiza los clientes BeeGFS

Después de actualizar con éxito tu clúster a BeeGFS v8, también tienes que actualizar todos los clientes BeeGFS.

Los siguientes pasos describen el proceso para actualizar los clientes BeeGFS en un sistema basado en Ubuntu.

1. Si aún no lo has hecho, detén el servicio cliente BeeGFS:

```
systemctl stop beegfs-client
```

2. Agrega el repositorio de paquetes BeeGFS v8 para tu distribución de Linux. Las instrucciones para usar los repositorios oficiales de BeeGFS se pueden encontrar en "[Página de descarga de BeeGFS](#)". De lo contrario, configura tu repositorio espejo local de BeeGFS según corresponda.

Los siguientes pasos usan el repositorio oficial de BeeGFS 8.2 en un sistema basado en Ubuntu:

3. Importa la clave GPG de BeeGFS:

```
wget https://www.beegfs.io/release/beegfs_8.2/gpg/GPG-KEY-beegfs -O /etc/apt/trusted.gpg.d/beegfs.asc
```

4. Descarga el archivo del repositorio:

```
wget https://www.beegfs.io/release/beegfs_8.2/dists/beegfs-noble.list -O /etc/apt/sources.list.d/beegfs.list
```



Elimina cualquier repositorio BeeGFS previamente configurado para evitar conflictos con el nuevo repositorio BeeGFS v8.

5. Actualiza los paquetes del cliente BeeGFS:

```
apt-get update  
apt-get install --only-upgrade beegfs-client
```

6. Configura TLS para el cliente. TLS es necesario para usar la CLI de BeeGFS. Consulta el procedimiento "[Configura el cifrado TLS para BeeGFS 8](#)" para configurar TLS en el cliente.
7. Inicia el servicio cliente BeeGFS:

```
systemctl start beegfs-client
```

Verifica la actualización

Después de terminar la actualización a BeeGFS v8, ejecuta los siguientes comandos para verificar que la actualización fue exitosa.

1. Verifica que el nodo de información raíz pertenezca al mismo nodo de metadatos que antes. Esto debería ocurrir automáticamente si usaste la funcionalidad `import-from-v7` en el servicio de gestión:

```
beegfs entry info /mnt/beegfs
```

2. Verifica que todos los nodos y objetivos estén en línea y en buen estado:

```
beegfs health check
```



Si la comprobación de "Capacidad disponible" advierte que los targets tienen poco espacio libre, puedes ajustar los umbrales del "capacity pool" definidos en el archivo `beegfs-mgmtd.toml` para que se adapten mejor a tu entorno.

Actualice los paquetes Pacemaker y Corosync en un clúster HA

Siga estos pasos para actualizar los paquetes Pacemaker y Corosync en un clúster HA.

Descripción general

La actualización de Pacemaker y Corosync garantiza que el clúster se beneficie de nuevas funciones, parches de seguridad y mejoras de rendimiento.

Enfoque de actualización

Hay dos enfoques recomendados para actualizar un clúster: Una actualización gradual o un apagado completo del clúster. Cada enfoque tiene sus propias ventajas y desventajas. El procedimiento de actualización puede variar en función de la versión de Pacemaker. Consulte la documentación de ClusterLabs "[Actualización de un grupo de marcapasos](#)" para determinar qué enfoque usar. Antes de seguir un enfoque de actualización, compruebe que:

- Los nuevos paquetes Pacemaker y Corosync son compatibles con la solución BeeGFS de NetApp.
- Existen copias de seguridad válidas para la configuración del sistema de archivos BeeGFS y del clúster Pacemaker.
- El clúster está en buen estado.

Actualización gradual

Este método implica eliminar cada nodo del clúster, actualizarlo y, a continuación, volver a introducirlo al clúster hasta que todos los nodos ejecuten la nueva versión. Este método mantiene el clúster operativo, lo

cual es ideal para clústeres de alta disponibilidad de mayor tamaño, pero conlleva el riesgo de ejecutar versiones mixtas durante el proceso. Este método debe evitarse en clústeres de dos nodos.

1. Confirme que el clúster tiene el estado óptimo y que cada servicio BeeGFS se ejecute en su nodo preferido. Consulte "[Examine el estado del clúster](#)" para obtener más información.
2. Para que el nodo se actualice, colóquelo en el modo de espera para drenar (o mover) todos los servicios de BeeGFS:

```
pcs node standby <HOSTNAME>
```

3. Compruebe que los servicios del nodo se han drenado ejecutando:

```
pcs status
```

Asegúrese de que no se informa de ningún servicio como Started en el nodo en espera.



Según el tamaño de su clúster, los servicios pueden tardar segundos o minutos en moverse al nodo hermano. Si un servicio BeeGFS no se inicia en el nodo hermano, consulte el "[Guías de solución de problemas](#)".

4. Apague el clúster en el nodo:

```
pcs cluster stop <HOSTNAME>
```

5. Actualice los paquetes Pacemaker, Corosync y pc en el nodo:



Los comandos del administrador de paquetes variarán según el sistema operativo. Los siguientes comandos son para sistemas que ejecutan RHEL 8 y posteriores.

```
dnf update pacemaker-<version>
```

```
dnf update corosync-<version>
```

```
dnf update pcs-<version>
```

6. Inicie los servicios de clúster de Pacemaker en el nodo:

```
pcs cluster start <HOSTNAME>
```

7. Si el `pcs` paquete se actualizó, vuelva a autenticar el nodo con el clúster:

```
pcs host auth <HOSTNAME>
```

8. Compruebe que la configuración del marcapasos sigue siendo válida con la `crm_verify` herramienta.



Esto solo debe verificarse una vez durante la actualización del clúster.

```
crm_verify -L -v
```

9. Saque el nodo del modo de espera:

```
pcs node unstandby <HOSTNAME>
```

10. Reubique todos los servicios de BeeGFS de nuevo en su nodo preferido:

```
pcs resource relocate run
```

11. Repita los pasos anteriores para cada nodo del cluster hasta que todos los nodos ejecuten las versiones de Pacemaker, Corosync y pc que desee.
12. Por último, ejecute `pcs status` y compruebe que el estado del clúster esté en buen estado y el Current DC informe la versión de Pacemaker que deseé.



Si los Current DC informan 'versión modificada', un nodo del cluster todavía se está ejecutando con la versión anterior de Pacemaker y debe actualizarse. Si algún nodo actualizado no puede volver a unirse al clúster o si los recursos no se inician, compruebe los registros del clúster y consulte las notas de la versión de Pacemaker o las guías de usuario para ver si hay problemas de actualización conocidos.

Complete el cierre del clúster

En este enfoque, todos los nodos y recursos del clúster están apagados, los nodos se actualizan y después se reinicia el clúster. Este enfoque es necesario si las versiones Pacemaker y Corosync no admiten una configuración de versiones mixtas.

1. Confirme que el clúster tiene el estado óptimo y que cada servicio BeeGFS se ejecute en su nodo preferido. Consulte "[Examine el estado del clúster](#)" para obtener más información.
2. Apague el software del clúster (Pacemaker y Corosync) en todos los nodos.



Según el tamaño del clúster, puede que todo el clúster tarde segundos o minutos en detenerse.

```
pcs cluster stop --all
```

3. Una vez que los servicios de cluster se hayan apagado en todos los nodos, actualice los paquetes de Pacemaker, Corosync y pc de cada nodo según sus requisitos.



Los comandos del administrador de paquetes variarán según el sistema operativo. Los siguientes comandos son para sistemas que ejecutan RHEL 8 y posteriores.

```
dnf update pacemaker-<version>
```

```
dnf update corosync-<version>
```

```
dnf update pcs-<version>
```

4. Después de actualizar todos los nodos, inicie el software del clúster en todos los nodos:

```
pcs cluster start --all
```

5. Si el pcs paquete se actualizó, vuelva a autenticar cada nodo del clúster:

```
pcs host auth <HOSTNAME>
```

6. Por último, ejecute `pcs status` y compruebe que el clúster esté en buen estado y que Current DC informe de la versión de Pacemaker correcta.



Si los Current DC informes 'versión modificada', un nodo del cluster todavía se está ejecutando con la versión anterior de Pacemaker y debe actualizarse.

Actualice el firmware del adaptador de nodo de archivo

Siga estos pasos para actualizar los adaptadores ConnectX-7 del nodo de archivo al firmware más reciente.

Descripción general

Es posible que sea necesario actualizar el firmware del adaptador ConnectX-7 para admitir un nuevo controlador MLNX_OFED, habilitar nuevas funciones o corregir errores. Esta guía utilizará la utilidad de NVIDIA `mlxfwmanager` para las actualizaciones de los adaptadores debido a su facilidad de uso y eficiencia.

Consideraciones de renovación

Esta guía cubre dos enfoques para actualizar el firmware del adaptador ConnectX-7: Una actualización gradual y una actualización de clústeres de dos nodos. Seleccione el enfoque de actualización adecuado según el tamaño del clúster. Antes de realizar actualizaciones de firmware, compruebe lo siguiente:

- Se ha instalado un controlador MLNX_OFED compatible; consulte la "[requisitos tecnológicos](#)".
- Existen copias de seguridad válidas para la configuración del sistema de archivos BeeGFS y del clúster Pacemaker.
- El clúster está en buen estado.

Preparación de la actualización del firmware

Se recomienda utilizar la utilidad de NVIDIA `mlxfwmanager` para actualizar el firmware del adaptador de un nodo, que se incluye con el controlador MLNX_OFED de NVIDIA. Antes de iniciar las actualizaciones, descargue la imagen de firmware del adaptador de "[Sitio de soporte de NVIDIA](#)" y almacénela en cada nodo de archivo.



Para los adaptadores Lenovo ConnectX-7, utilice la `mlxfwmanager_LES` herramienta, que está disponible en la página de NVIDIA "[Firmware de OEM](#)".

Enfoque de actualización gradual

Este enfoque se recomienda para cualquier clúster de alta disponibilidad con más de dos nodos. Este enfoque implica actualizar el firmware del adaptador en un nodo de archivos cada vez, lo que permite que el clúster de alta disponibilidad mantenga solicitudes de servicio, aunque se recomienda evitar el mantenimiento de I/O durante este momento.

1. Confirme que el clúster tiene el estado óptimo y que cada servicio BeeGFS se ejecute en su nodo preferido. Consulte "[Examine el estado del clúster](#)" para obtener más información.
2. Elija un nodo de archivo para actualizar y colóquelo en modo de espera, lo que drena (o mueve) todos los servicios BeeGFS de ese nodo:

```
pcs node standby <HOSTNAME>
```

3. Compruebe que los servicios del nodo se han drenado ejecutando:

```
pcs status
```

Compruebe que ningún servicio está informando como `Started` en el nodo en espera.



Según el tamaño del clúster, los servicios de BeeGFS pueden tardar segundos o minutos en moverse al nodo hermano. Si un servicio BeeGFS no se inicia en el nodo hermano, consulte el "[Guías de solución de problemas](#)".

4. Actualice el firmware del adaptador con `mlxfwmanager`.

```
mlxfwmanager -i <path/to/firmware.bin> -u
```

Tenga en cuenta la `PCI Device Name` para cada adaptador que recibe actualizaciones de firmware.

5. Restablezca cada adaptador mediante la `mlxfwreset` utilidad para aplicar el nuevo firmware.



Algunas actualizaciones de firmware pueden requerir un reinicio para aplicar la actualización. Consulte "["Limitaciones de mlxfwreset de NVIDIA"](#)" para obtener instrucciones. Si se requiere un reinicio, reinicie los adaptadores en lugar de restablecerlos.

- a. Detenga el servicio opensm:

```
systemctl stop opensm
```

- b. Ejecute el siguiente comando para cada una de las PCI Device Name notas anteriores.

```
mlxfwreset -d <pci_device_name> reset -y
```

- c. Inicie el servicio opensm:

```
systemctl start opensm
```

- d. Reiniciar el eseries_nvme_ib.service .

```
systemctl restart eseries_nvme_ib.service
```

- e. Verifique que los volúmenes de la matriz de almacenamiento de la Serie E estén presentes.

```
multipath -ll
```

1. Ejecute ibstat y verifique que todos los adaptadores estén funcionando en la versión de firmware deseada:

```
ibstat
```

2. Inicie los servicios de clúster de Pacemaker en el nodo:

```
pcs cluster start <HOSTNAME>
```

3. Saque el nodo del modo de espera:

```
pcs node unstandby <HOSTNAME>
```

4. Reubique todos los servicios de BeeGFS de nuevo en su nodo preferido:

```
pcs resource relocate run
```

Repita estos pasos para cada nodo de archivo del clúster hasta que se hayan actualizado todos los adaptadores.

Método de actualización de clústeres de dos nodos

Este método se recomienda para clústeres de alta disponibilidad con solo dos nodos. Este enfoque es similar a una actualización gradual, pero incluye pasos adicionales para evitar tiempos de inactividad del servicio cuando se detienen los servicios de clúster de un nodo.

1. Confirme que el clúster tiene el estado óptimo y que cada servicio BeeGFS se ejecute en su nodo preferido. Consulte "[Examine el estado del clúster](#)" para obtener más información.
2. Seleccione un nodo de archivo para actualizar y coloque el nodo en modo de espera, lo que drena (o mueve) todos los servicios BeeGFS de ese nodo:

```
pcs node standby <HOSTNAME>
```

3. Compruebe que los recursos del nodo se han drenado ejecutando:

```
pcs status
```

Compruebe que ningún servicio está informando como `Started` en el nodo en espera.



Según el tamaño del clúster, los servicios de BeeGFS pueden tardar segundos o minutos en informar como en `Started` el nodo hermano. Si un servicio BeeGFS no se inicia, consulte la "[Guías de solución de problemas](#)".

4. Coloque el clúster en modo de mantenimiento.

```
pcs property set maintenance-mode=true
```

5. Actualice el firmware del adaptador con `mlxfwmanager`.

```
mlxfwmanager -i <path/to/firmware.bin> -u
```

Tenga en cuenta la `PCI Device Name` para cada adaptador que recibe actualizaciones de firmware.

6. Restablezca cada adaptador mediante la `mlxfwreset` utilidad para aplicar el nuevo firmware.



Algunas actualizaciones de firmware pueden requerir un reinicio para aplicar la actualización. Consulte "[Limitaciones de mlxfwreset de NVIDIA](#)" para obtener instrucciones. Si se requiere un reinicio, reinicie los adaptadores en lugar de restablecerlos.

a. Detenga el servicio opensm:

```
systemctl stop opensm
```

b. Ejecute el siguiente comando para cada una de las PCI Device Name notas anteriores.

```
mlxfwreset -d <pci_device_name> reset -y
```

c. Inicie el servicio opensm:

```
systemctl start opensm
```

7. Ejecute ibstat y verifique que todos los adaptadores estén funcionando en la versión de firmware deseada:

```
ibstat
```

8. Inicie los servicios de clúster de Pacemaker en el nodo:

```
pcs cluster start <HOSTNAME>
```

9. Saque el nodo del modo de espera:

```
pcs node unstandby <HOSTNAME>
```

10. Saque el clúster del modo de mantenimiento.

```
pcs property set maintenance-mode=false
```

11. Reubique todos los servicios de BeeGFS de nuevo en su nodo preferido:

```
pcs resource relocate run
```

Repita estos pasos para cada nodo de archivo del clúster hasta que se hayan actualizado todos los adaptadores.

Actualice la cabina de almacenamiento E-Series

Siga estos pasos para actualizar los componentes de la cabina de almacenamiento E-

Series del clúster HA.

Descripción general

Mantener las cabinas de almacenamiento de NetApp E-Series del clúster de alta disponibilidad actualizadas con el firmware más reciente garantiza un rendimiento óptimo y una mayor seguridad. Las actualizaciones de firmware para la cabina de almacenamiento se aplican a través de sistema operativo SANtricity, NVSRAM y archivos de firmware de la unidad.



Aunque las cabinas de almacenamiento se pueden actualizar con el clúster de alta disponibilidad en línea, se recomienda colocar el clúster en modo de mantenimiento para todas las actualizaciones.

Pasos de actualización del nodo de bloque

Los siguientes pasos describen cómo actualizar el firmware de las cabinas de almacenamiento mediante `Netapp_Eseries.Santricity` la colección Ansible. Antes de continuar, revise "["Consideraciones de renovación"](#)" para actualizar los sistemas E-Series.



Solo es posible actualizar a SANtricity OS 11.80 o versiones posteriores desde 11.70.5P1. Primero, la cabina de almacenamiento debe actualizarse a 11.70.5P1 antes de aplicar nuevas actualizaciones.

1. Valide que el nodo de control de Ansible utilice la colección de Ansible más reciente de SANtricity.
 - Para actualizaciones de colecciones con acceso a. "["Galaxia de ansible"](#)", ejecute el siguiente comando:

```
ansible-galaxy collection install netapp_eseries.santricity --upgrade
```
 - Para actualizaciones sin conexión, descargue el tarball de recopilación de "["Galaxia de ansible"](#)", transfíralo al nodo de control y ejecute:

```
ansible-galaxy collection install netapp_eseries-santricity-<VERSION>.tar.gz --upgrade
```
2. Obtenga el firmware más reciente para la cabina de almacenamiento y las unidades.
 - a. Descargue los archivos de firmware.
 - **Sistema operativo SANtricity y NVSRAM:** Navegue hasta la "["Sitio de soporte de NetApp"](#)" versión más reciente de SANtricity OS y NVSRAM para su modelo de cabina de almacenamiento y descargue la versión más reciente de NVSRAM.
 - **Firmware de la unidad:** Navegue hasta "["Sitio del firmware de un disco E-Series"](#)" y descargue el firmware más reciente para cada uno de los modelos de unidad de la cabina de almacenamiento.
 - b. Almacene los archivos de firmware del sistema operativo SANtricity, NVSRAM y la unidad en `<inventory_directory>/packages` el directorio del nodo de control Ansible.
3. Si es necesario, actualice los archivos de inventario de Ansible del clúster para incluir todas las cabinas de almacenamiento (nodos de bloque) que requieran actualizaciones. Para obtener orientación, consulte la

"Descripción general del inventario de Ansible" sección.

4. Compruebe que el clúster tenga un estado óptimo con cada servicio de BeeGFS en el nodo preferido. Consulte ["Examine el estado del clúster"](#) para obtener más información.
5. Coloque el clúster en modo de mantenimiento siguiendo las instrucciones que se indican en ["Coloque el clúster en modo de mantenimiento"](#).
6. Cree un nuevo libro de estrategia de Ansible llamado `update_block_node_playbook.yml`. Complete el libro de estrategia con el siguiente contenido, sustituyendo las versiones del sistema operativo SANtricity, NVSRAM y firmware de la unidad a la ruta de actualización que desee:

```
- hosts: eseries_storage_systems
gather_facts: false
any_errors_fatal: true
collections:
  - netapp_eseries.santricity
vars:
  eseries_firmware_firmware: "packages/<SantricityOS>.dlp"
  eseries_firmware_nvram: "packages/<NVSRAM>.dlp"
  eseries_drive_firmware_firmware_list:
    - "packages/<drive_firmware>.dlp"
  eseries_drive_firmware_upgrade_drives_online: true

tasks:
  - name: Configure NetApp E-Series block nodes.
    import_role:
      name: nar_santricity_management
```

7. Para iniciar las actualizaciones, ejecute el siguiente comando desde el nodo de control de Ansible:

```
ansible-playbook -i inventory.yml update_block_node_playbook.yml
```

8. Una vez que se complete el libro de estrategia, compruebe que cada cabina de almacenamiento tenga el estado Óptimo.
9. Mueva el clúster fuera del modo de mantenimiento y compruebe que el clúster tenga el estado óptimo con cada servicio BeeGFS en su nodo preferido.

Mantenimiento y mantenimiento

Servicios de conmutación por error y conmutación tras recuperación

Desplazamiento de servicios BeeGFS entre nodos del clúster.

Descripción general

Los servicios BeeGFS pueden realizar una conmutación por error entre los nodos del clúster para garantizar que los clientes puedan continuar accediendo al sistema de archivos si un nodo experimenta un error o

necesita realizar tareas de mantenimiento planificadas. En esta sección se describen distintas formas en las que los administradores pueden recuperar el clúster después de un fallo o mover manualmente servicios entre nodos.

Pasos

Comutación por error y conmutación por recuperación

Comutación al respaldo (planificada)

En general, cuando necesite desconectar un solo nodo de archivos para realizar el mantenimiento, querrá mover (o drenar) todos los servicios de BeeGFS de ese nodo. Esto se puede lograr poniendo el nodo en espera en primer lugar:

```
pcs node standby <HOSTNAME>
```

Después de verificar utilizando `pcs status` todos los recursos se han reiniciado en el nodo de archivos alternativo, puede apagar o realizar otros cambios en el nodo según sea necesario.

Comutación tras recuperación (después de una conmutación al respaldo planificada)

Cuando esté listo para restaurar los servicios BeeGFS en el nodo preferido, ejecute primero `pcs status` Y verifique en la "Lista de nodos" el estado es en espera. Si el nodo se reinició, aparecerá sin conexión hasta que los servicios del clúster estén en línea:

```
pcs cluster start <HOSTNAME>
```

Una vez que el nodo esté en línea, salga del modo de espera con:

```
pcs node unstandby <HOSTNAME>
```

Por último, reubique todos los servicios de BeeGFS en sus nodos preferidos con:

```
pcs resource relocate run
```

Comutación tras recuperación (después de una conmutación al respaldo no planificada)

Si un nodo experimenta un fallo de hardware o de otro tipo, el clúster de alta disponibilidad debería reaccionar automáticamente y mover sus servicios a un nodo en buen estado, lo que proporciona tiempo para que los administradores tomen acciones correctivas. Antes de continuar, consulte la "[resolución de problemas](#)" sección para determinar la causa de la conmutación por error y resolver los problemas pendientes. Una vez que el nodo se vuelve a encender y en buen estado, puede continuar con la conmutación tras recuperación.

Cuando un nodo se arranca tras un reinicio no planificado (o planificado), los servicios de clúster no se establecen para iniciarse automáticamente, por lo que primero tendrá que conectar el nodo con:

```
pcs cluster start <HOSTNAME>
```

A continuación, borre los errores de los recursos y restablezca el historial de cercas del nodo:

```
pcs resource cleanup node=<HOSTNAME>
pcs stonith history cleanup <HOSTNAME>
```

Verifique en `pcs status` el nodo está en línea y en buen estado. De forma predeterminada, los servicios de BeeGFS no se podrán recuperar automáticamente para evitar que los recursos vuelvan a un nodo que no esté en buenas estado. Cuando esté listo, devuelva todos los recursos del clúster a los nodos preferidos con:

```
pcs resource relocate run
```

Mover servicios de BeeGFS individuales a nodos de archivo alternativos

Mueva permanentemente un servicio BeeGFS a un nuevo nodo de archivo

Si desea cambiar de forma permanente el nodo de archivo preferido de un servicio BeeGFS individual, ajuste el inventario de Ansible para ver primero el nodo preferido y volver a ejecutar el libro de estrategia de Ansible.

Por ejemplo, en este archivo de ejemplo `inventory.yml`, `beegfs_01` es el nodo de archivos preferido para ejecutar el servicio de gestión BeeGFS:

```
mgmt:
  hosts:
    beegfs_01:
    beegfs_02:
```

Si se invierte el pedido, se preferirían los servicios de gestión en `beegfs_02`:

```
mgmt:
  hosts:
    beegfs_02:
    beegfs_01:
```

Mueva temporalmente un servicio BeeGFS a otro nodo de archivo

Generalmente, si un nodo está en proceso de mantenimiento, deberá utilizar los [pasos de conmutación por error y conmutación por recuperación](#failover-and-failback) para mover todos los servicios fuera de ese nodo.

Si por algún motivo necesita mover un servicio individual a un nodo de archivo diferente ejecutado:

```
pcs resource move <SERVICE> -monitor <HOSTNAME>
```



No especifique recursos individuales ni el grupo de recursos. Especifique siempre el nombre del monitor para el servicio BeeGFS que desea reubicar. Por ejemplo, para mover el servicio de gestión BeeGFS a beegfs_02 ejecute: `pcs resource move mgmt-monitor beegfs_02`. Este proceso se puede repetir para mover uno o varios servicios de sus nodos preferidos. Verifique que `pcs status` los servicios se han reubicado/iniciado en el nuevo nodo.

Para devolver un servicio BeeGFS a su nodo preferido, borre primero las restricciones de recursos temporales (repita este paso según sea necesario para varios servicios):

```
pcs resource clear <SERVICE>-monitor
```

A continuación, cuando esté listo para mover realmente los servicios de nuevo a sus nodos preferidos ejecutar:

```
pcs resource relocate run
```

Nota este comando reubicará los servicios que ya no tengan restricciones temporales de recursos que no estén en sus nodos preferidos.

Coloque el clúster en modo de mantenimiento

Evite que el clúster de alta disponibilidad reaccione accidentalmente a los cambios previstos del entorno.

Descripción general

Si pone el clúster en el modo de mantenimiento, se deshabilita toda la supervisión de recursos y se impide que Pacemaker mueva o gestione los recursos del clúster de algún otro modo. Todos los recursos permanecerán en ejecución en sus nodos originales, independientemente de que haya una condición de fallo temporal que impida que se pueda acceder a ellos. Los escenarios en los que esto es recomendable/útil incluyen:

- Mantenimiento de red que puede interrumpir temporalmente las conexiones entre nodos de archivo y servicios BeeGFS.
- Actualizaciones de nodos de bloques.
- Actualizaciones del sistema operativo, el kernel u otros paquetes del nodo de archivos.

Por lo general, el único motivo para poner manualmente el clúster en modo de mantenimiento es impedir que este reaccione a cambios externos en el entorno. Si un nodo individual del clúster requiere reparación física no utilice modo de mantenimiento y simplemente coloque ese nodo en espera tras el procedimiento anterior. Tenga en cuenta que el nuevo enrutamiento de Ansible pondrá automáticamente el clúster en modo de mantenimiento para facilitar la mayoría de las tareas de mantenimiento de software, incluidas las actualizaciones y los cambios de configuración.

Pasos

Para comprobar si el clúster se encuentra en modo de mantenimiento ejecutar:

```
pcs property config
```

`maintenance-mode` La propiedad no aparecerá si el cluster funciona normalmente. Si el cluster está actualmente en modo de mantenimiento, la propiedad se informará como `true`. Para habilitar la ejecución del modo de mantenimiento:

```
pcs property set maintenance-mode=true
```

Puede verificar ejecutando el estado del pc y asegurando que todos los recursos muestren "(no administrado)". Para desconectar el clúster del modo de mantenimiento ejecute:

```
pcs property set maintenance-mode=false
```

Detenga e inicie el clúster

Detener e iniciar correctamente el clúster de alta disponibilidad.

Descripción general

En esta sección se describe cómo apagar y reiniciar correctamente el clúster BeeGFS. Algunos ejemplos de casos en los que esto puede ser necesario son el mantenimiento eléctrico o la migración entre centros de datos o racks.

Pasos

Si por algún motivo necesita detener todo el clúster BeeGFS y apagar todos los servicios que se ejecutan:

```
pcs cluster stop --all
```

También es posible detener el clúster en nodos individuales (que automáticamente conmutarán por error los servicios a otro nodo), aunque se recomienda poner primero el nodo en espera (consulte la "[conmutación al respaldo](#)" sección):

```
pcs cluster stop <HOSTNAME>
```

Para iniciar los servicios y recursos del clúster en todos los nodos ejecutados:

```
pcs cluster start --all
```

O inicie servicios en un nodo específico con:

```
pcs cluster start <HOSTNAME>
```

En este momento, corre `pcs status` Compruebe que el clúster y los servicios BeeGFS se inicien en todos los nodos y que los servicios se estén ejecutando en los nodos que espera.



En función del tamaño del cluster, puede que todo el cluster tarde unos segundos o minutos en detenerse, o en mostrarse como iniciado en `pcs status`. Si `pcs cluster <COMMAND>` se bloquea durante más de cinco minutos, antes de ejecutar Ctrl+C para cancelar el comando, inicie sesión en cada nodo del cluster y utilice `pcs status` para ver si los servicios de cluster (Corosync/Pacemaker) siguen ejecutándose en ese nodo. Desde cualquier nodo en el que el clúster siga estando activo, puede comprobar qué recursos están bloqueando el clúster. Solucione manualmente el problema y el comando debería estar completo o se puede volver a ejecutar para detener el resto de servicios.

Sustituya los nodos de archivo

Reemplazar un nodo de archivo si el servidor original está defectuoso.

Descripción general

Esta es una descripción general de los pasos necesarios para reemplazar un nodo de archivo del clúster. Estos pasos suponen un error en el nodo de archivo debido a un problema de hardware y se reemplazaron por un nuevo nodo de archivo idéntico.

Pasos:

1. Sustituya físicamente el nodo de archivo y restaure todo el cableado al nodo de bloque y a la red de almacenamiento.
2. Vuelva a instalar el sistema operativo en el nodo de archivos, incluida la adición de suscripciones a Red Hat.
3. Configure la gestión y las redes de BMC en el nodo de archivo.
4. Actualice el inventario de Ansible si el nombre de host, la IP, las asignaciones de interfaz de PCIe a lógica o cualquier otro cambio relacionado con el nodo de archivo nuevo. Generalmente, esto no es necesario si el nodo se reemplazó con un hardware de servidor idéntico y si utiliza la configuración de red original.
 - a. Por ejemplo, si el nombre de host ha cambiado, cree (o cambie de nombre) el archivo de inventario del nodo (`host_vars/<NEW_NODE>.yml``) Luego en el archivo de inventario de Ansible (`inventory.yml`), reemplace el nombre del nodo antiguo por el nuevo nombre del nodo:

```

all:
  ...
  children:
    ha_cluster:
      children:
        mgmt:
          hosts:
            node_h1_new:    # Replaced "node_h1" with "node_h1_new"
            node_h2:

```

5. De uno de los otros nodos del clúster, quite el nodo antiguo: `pcs cluster node remove <HOSTNAME>`.



NO CONTINÚE ANTES DE EJECUTAR ESTE PASO.

6. En el nodo de control Ansible:

- a. Quite la clave SSH antigua con:

```
`ssh-keygen -R <HOSTNAME_OR_IP>`
```

- b. Configure SSH sin contraseña al nodo de sustitución con:

```
ssh-copy-id <USER>@<HOSTNAME_OR_IP>
```

7. Vuelva a ejecutar el libro de estrategia de Ansible para configurar el nodo y añadirlo al clúster:

```
ansible-playbook -i <inventory>.yml <playbook>.yml
```

8. En este momento, corre `pcs status` y compruebe que el nodo sustituido ahora aparece y ejecuta servicios.

Expanda o reduzca el clúster

Añada o quite bloques de creación del clúster.

Descripción general

En esta sección se documentan varias consideraciones y opciones para ajustar el tamaño del clúster de alta disponibilidad de BeeGFS. Normalmente, el tamaño del clúster se ajusta agregando o quitando elementos básicos, que normalmente son dos nodos de archivo configurados como un par de alta disponibilidad. También es posible agregar o quitar nodos de archivos individuales (u otros tipos de nodos de clústeres) si es necesario.

Añadir una elemento básico al clúster

Consideraciones

El crecimiento del clúster mediante la adición de elementos básicos adicionales es un proceso sencillo. Antes de empezar a tener en cuenta las restricciones en torno al número mínimo y máximo de nodos de clúster en cada clúster de alta disponibilidad, y determinar si debe añadir nodos al clúster de alta disponibilidad existente o crear un nuevo clúster de alta disponibilidad. Normalmente, cada bloque de creación consta de dos nodos de archivo, pero tres nodos son el número mínimo de nodos por clúster (para establecer quórum), y diez son el máximo recomendado (probado). En situaciones avanzadas es posible añadir un solo nodo "tiebreaker" que no ejecute ningún servicio BeeGFS al poner en marcha un clúster de dos nodos. Póngase en contacto con el servicio de soporte de NetApp si está considerando realizar dicha implementación.

Tenga en cuenta estas restricciones y cualquier crecimiento futuro del clúster anticipado al decidir cómo ampliar el clúster. Por ejemplo, si tiene un clúster de seis nodos y necesita añadir cuatro nodos más, se recomienda simplemente iniciar un nuevo clúster de alta disponibilidad.

 Recuerde que un solo sistema de archivos BeeGFS puede consistir en varios clústeres de alta disponibilidad independientes. Esto permite que los sistemas de archivos sigan escalando entre los límites de hardware recomendado y los componentes de clúster de alta disponibilidad subyacentes.

Pasos

Al agregar un elemento básico al clúster, deberá crear los `host_vars` archivos para cada uno de los nuevos nodos de archivo y los nodos de bloque (cabinas E-Series). Los nombres de estos hosts deben agregarse al inventario, junto con los nuevos recursos que se van a crear. `group_vars` Se deberán crear los archivos correspondientes para cada nuevo recurso. Consulte la "[utilizar arquitecturas personalizadas](#)" sección para obtener más información.

Una vez creados los archivos correctos, todo lo que se necesita es volver a ejecutar la automatización mediante el comando:

```
ansible-playbook -i <inventory>.yml <playbook>.yml
```

Eliminación de un elemento básico del clúster

Hay una serie de consideraciones que tener en cuenta cuando se necesita retirar un bloque de construcción, por ejemplo:

- ¿Qué servicios BeeGFS se están ejecutando en este bloque de creación?
- ¿Solo se retiran los nodos de archivos y los nodos de bloque deben adjuntarse a nuevos nodos de archivos?
- Si se retira todo el elemento básico, ¿deben moverse los datos a un nuevo elemento básico, dispersarse en nodos existentes en el clúster o moverse a un nuevo sistema de archivos BeeGFS u otro sistema de almacenamiento?
- ¿Puede suceder esto durante una interrupción o se debe realizar de forma no disruptiva?
- ¿El elemento básico se está utilizando de forma activa o contiene principalmente datos que ya no están activos?

Debido a la diversidad de puntos de partida posibles y a los estados finales deseados, póngase en contacto

con el soporte de NetApp para que podamos identificar y ayudar a implementar la mejor estrategia en función de su entorno y sus requisitos.

Solucionar problemas

Solucionar problemas de un clúster de alta disponibilidad de BeeGFS.

Descripción general

En esta sección se explica cómo investigar y solucionar varios fallos y otros escenarios que pueden surgir al utilizar un clúster de alta disponibilidad de BeeGFS.

Guías de solución de problemas

Investigando conmutaciones al respaldo inesperadas

Cuando un nodo tiene una barrera aplicada de forma inesperada y sus servicios pasan a otro nodo, el primer paso debe ser comprobar si el clúster indica algún error de recurso en la parte inferior de `pcs status`. Por lo general, no habrá nada presente si la delimitación se ha realizado correctamente y se han reiniciado los recursos en otro nodo.

Por lo general, el siguiente paso será buscar a través de los registros del sistema utilizando `journalctl`. En cualquiera de los nodos de archivo restantes (los registros de Pacemaker se sincronizan en todos los nodos). Si sabe la hora en que ocurrió el fallo, puede iniciar la búsqueda justo antes de que se produjera el fallo (generalmente se recomienda al menos diez minutos antes):

```
journalctl --since "<YYYY-MM-DD HH:MM:SS>"
```

En las siguientes secciones se muestra el texto común que se puede obtener en los registros para delimitar aún más la investigación.

Pasos para investigar/resolver

Paso 1: Compruebe si el monitor BeeGFS ha detectado un fallo:

Si el monitor BeeGFS ha activado la conmutación por error, debería aparecer un error (si no es así, continúe con el siguiente paso).

```
journalctl --since "<YYYY-MM-DD HH:MM:SS>" | grep -i unexpected
[...]
Jul 01 15:51:03 beegfs_01 pacemaker-schedulerd[9246]: warning: Unexpected
result (error: BeeGFS service is not active!) was recorded for monitor of
meta_08-monitor on beegfs_02 at Jul 1 15:51:03 2022
```

En esta instancia, el servicio de BeeGFS meta_08 se detuvo por algún motivo. Para continuar con la solución de problemas, debemos iniciar beegfs_02 y revisar los registros del servicio en `/var/log/beegfs-meta-meta_08_tgt_0801.log`. Por ejemplo, el servicio BeeGFS puede haber encontrado un error de aplicación debido a un problema interno o al nodo.



A diferencia de los registros de Pacemaker, los registros de los servicios BeeGFS no se distribuyen a todos los nodos del clúster. Para investigar estos tipos de errores, son necesarios los registros del nodo original en el que se produjo el error.

Entre los posibles problemas que podría generar el monitor se incluyen los siguientes:

- No se puede acceder a los destinos.
 - Descripción: Indica que no se puede acceder a los volúmenes de bloques.
 - Solución de problemas:
 - Si también no se pudo iniciar el servicio en el nodo de archivos alternativo, confirme que el nodo de bloque está en buen estado.
 - Compruebe si hay problemas físicos que impidan el acceso a los nodos de bloque desde este nodo de archivos, por ejemplo, adaptadores o cables InfiniBand defectuosos.
- ¡No se puede acceder a la red!
 - Descripción: Ninguno de los adaptadores utilizados por los clientes para conectarse a este servicio BeeGFS estaba en línea.
 - Solución de problemas:
 - Si varios o todos los nodos de archivo se vieron afectados, compruebe si se produjo un error en la red utilizada para conectar los clientes BeeGFS y el sistema de archivos.
 - Compruebe si hay problemas físicos que impidan el acceso a los clientes desde este nodo de archivos, por ejemplo, adaptadores o cables InfiniBand defectuosos.
- El servicio BeeGFS no está activo.
 - Descripción: Un servicio BeeGFS se ha detenido inesperadamente.
 - Solución de problemas:
 - En el nodo de archivo que notificó el error, compruebe los registros del servicio BeeGFS afectado para ver si se produjo un fallo. Si esto sucede, abra un caso con el soporte de NetApp para que pueda investigar el bloqueo.
 - Si no se ha informado de errores en el registro de BeeGFS, compruebe los registros del diario para ver si systemd ha registrado un motivo por el que se ha detenido el servicio. En algunos casos, es posible que el servicio BeeGFS no haya recibido la oportunidad de registrar ningún mensaje antes de que se terminara el proceso (por ejemplo, si se ejecutó a alguien) `kill -9 <PID>`).

Paso 2: Compruebe si el nodo dejó el clúster de forma inesperada

En caso de que el nodo sufriera un error de hardware catastrófico (por ejemplo, murió la placa del sistema) o se produjo un error de alerta en el kernel o un problema de software similar, el monitor BeeGFS no informará de este error. En su lugar, busque el nombre de host y debería ver mensajes del Pacemaker que indican que el nodo se ha perdido inesperadamente:

```
journalctl --since "<YYYY-MM-DD HH:MM:SS>" | grep -i <HOSTNAME>
[...]
Jul 01 16:18:01 beegfs_01 pacemaker-attrd[9245]: notice: Node beegfs_02
state is now lost
Jul 01 16:18:01 beegfs_01 pacemaker-controld[9247]: warning:
Stonith/shutdown of node beegfs_02 was not expected
```

Paso 3: Verifique que Pacemaker pudo cercar el nodo

En todos los escenarios debería ver que Pacemaker intenta cercar el nodo para verificar que está realmente sin conexión (los mensajes exactos pueden variar según la causa del cercado):

```
Jul 01 16:18:02 beegfs_01 pacemaker-schedulerd[9246]: warning: Cluster
node beegfs_02 will be fenced: peer is no longer part of the cluster
Jul 01 16:18:02 beegfs_01 pacemaker-schedulerd[9246]: warning: Node
beegfs_02 is unclean
Jul 01 16:18:02 beegfs_01 pacemaker-schedulerd[9246]: warning: Scheduling
Node beegfs_02 for STONITH
```

Si la acción de cercado se completa correctamente, verá mensajes como:

```
Jul 01 16:18:14 beegfs_01 pacemaker-fenced[9243]: notice: Operation 'off'
[2214070] (call 27 from pacemaker-controld.9247) for host 'beegfs_02' with
device 'fence_redfish_2' returned: 0 (OK)
Jul 01 16:18:14 beegfs_01 pacemaker-fenced[9243]: notice: Operation 'off'
targeting beegfs_02 on beegfs_01 for pacemaker-
controld.9247@beegfs_01.786df3a1: OK
Jul 01 16:18:14 beegfs_01 pacemaker-controld[9247]: notice: Peer
beegfs_02 was terminated (off) by beegfs_01 on behalf of pacemaker-
controld.9247: OK
```

Si la acción de delimitación falló por algún motivo, los servicios BeeGFS no podrán reiniciarse en otro nodo para evitar el riesgo de corrupción de datos. Eso sería un problema para investigar por separado, si, por ejemplo, el dispositivo de cercado (PDU o BMC) era inaccesible o mal configurado.

Acciones de recursos fallidos de direcciones (que se encuentran en la parte inferior del estado de los pc)

Si falla un recurso necesario para ejecutar un servicio BeeGFS, el monitor BeeGFS activará una conmutación por error. Si esto ocurre, es probable que no haya ninguna lista de acciones de recursos fallidas en la parte inferior de `pcs status` y debe consultar los pasos sobre cómo "[conmutación tras recuperación tras fallos no planificada](#)".

De lo contrario, normalmente sólo deberían haber dos escenarios en los que verá "acciones de recursos fallidas".

Pasos para investigar/resolver

Escenario 1: Se detectó un problema temporal o permanente con un agente de esgrima y se reinició u movió a otro nodo.

Algunos agentes de cercado son más confiables que otros, y cada uno implementará su propio método de monitoreo para garantizar que el dispositivo de cercado esté listo. En particular, el agente de esgrima de Redfish ha sido visto para informar de acciones de recursos fallidas como las siguientes, aunque todavía se muestre iniciado:

```
* fence_redfish_2_monitor_60000 on beegfs_01 'not running' (7):  
call=2248, status='complete', exitreason='', last-rc-change='2022-07-26  
08:12:59 -05:00', queued=0ms, exec=0ms
```

No se espera que un agente de delimitación que informe sobre acciones de recursos fallidas en un determinado nodo active una conmutación por error de los servicios BeeGFS que se ejecutan en ese nodo. Solo hay que reiniciar automáticamente en un mismo nodo o en uno distinto.

Pasos para resolver:

1. Si el agente de cercado se niega sistemáticamente a ejecutarse en todos los nodos o en un subconjunto de ellos, compruebe si dichos nodos pueden conectarse al agente de cercado y compruebe que el agente de cercado esté configurado correctamente en el inventario de Ansible.
 - a. Por ejemplo, si un agente de cercado Redfish (BMC) se está ejecutando en el mismo nodo que es responsable de cercado, y la gestión del SO y las IP de BMC están en la misma interfaz física, algunas configuraciones de switches de red no permitirán la comunicación entre las dos interfaces (para evitar bucles de red). De forma predeterminada, el clúster de alta disponibilidad intentará evitar colocar agentes de cercado en el nodo que sean responsables de cercado, pero esto puede suceder en algunos escenarios/configuraciones.
2. Una vez que se resuelven todos los problemas (o si el problema parece efímero), ejecute `pcs resource cleanup` para restablecer las acciones de recursos fallidas.

Escenario 2: El monitor BeeGFS detectó un problema y activó un fallo, pero por algún motivo los recursos no se pudieron iniciar en un nodo secundario.

Siempre que la delimitación esté habilitada y que el recurso no se haya bloqueado para detenerse en el nodo original (consulte la sección de solución de problemas "standby (on-fail)"), los motivos más probables incluyen problemas para iniciar el recurso en un nodo secundario debido a lo siguiente:

- El nodo secundario ya estaba desconectado.
- Un problema de configuración física o lógica impidió que el secundario acceda a los volúmenes de bloques utilizados como destinos de BeeGFS.

Pasos para resolver:

1. Para cada entrada de las acciones de recursos fallidas:
 - a. Confirme que la acción de recurso fallida fue una operación de inicio.
 - b. Según el recurso indicado y el nodo especificado en las acciones de recursos con errores:
 - i. Busque y corrija los problemas externos que podrían impedir que el nodo inicie el recurso especificado. Por ejemplo, si no se pudo iniciar la dirección IP de BeeGFS (IP flotante), compruebe

que al menos una de las interfaces necesarias está conectada/conectada y cableada al conmutador de red correcto. Si se produce un error en un objetivo de BeeGFS (dispositivo de bloque/volumen de E-Series), compruebe que las conexiones físicas con los nodos de bloque back-end estén conectadas según lo esperado y verifique que los nodos de bloque estén en buen estado.

- c. Si no hay problemas externos obvios y desea un motivo raíz para este incidente, se recomienda abrir un caso con la compatibilidad de NetApp para investigar antes de continuar, ya que los siguientes pasos pueden hacer que sea un desafío/imposible el análisis de causa raíz (RCA).
2. Después de resolver cualquier problema externo:
 - a. Comente cualquier nodo no funcional del archivo Ansible Inventory.yml y vuelva a ejecutar el libro de estrategia de Ansible completo para garantizar que toda la configuración lógica se configure correctamente en los nodos secundarios.
 - i. Nota: No olvide dejar de comentar estos nodos y volver a ejecutar la tabla playbook una vez que el estado de los nodos sea bueno y esté listo para realizar la conmutación tras recuperación.
 - b. También puede intentar recuperar manualmente el clúster:
 - i. Vuelva a colocar todos los nodos sin conexión en línea mediante: `pcs cluster start <HOSTNAME>`
 - ii. Borre todas las acciones de recursos fallidas mediante: `pcs resource cleanup`
 - iii. Ejecute el estado del pc y verifique que todos los servicios comiencen según lo esperado.
 - iv. Si es necesario, corre `pcs resource relocate run` para devolver los recursos a su nodo preferido (si está disponible).

Cuestiones comunes

Los servicios de BeeGFS no realizan una conmutación por error ni una conmutación tras recuperación cuando se le solicite

Asunto probable: la `pcs resource relocate` se ejecutó el comando de ejecución, pero nunca se terminó correctamente.

Cómo comprobar: Ejecutar `pcs constraint --full` Y compruebe si existen restricciones de ubicación con un ID de `pcs-relocate-<RESOURCE>`.

Cómo resolver: Ejecutar `pcs resource relocate clear` a continuación, vuelva a ejecutar `pcs constraint --full` para verificar que se han eliminado las restricciones adicionales.

Un nodo en el estado del pc muestra "standby (on-fail)" cuando está desactivado el cercado

Problema probable: Pacemaker no pudo confirmar con éxito todos los recursos fueron detenidos en el nodo que falló.

Cómo resolver:

1. Ejecución `pcs status` y busque los recursos que no se "hayan iniciado" o que muestren errores en la parte inferior del resultado y resuelva cualquier problema.
2. Para volver a poner en línea el nodo `pcs resource cleanup --node=<HOSTNAME>`.

Después de una conmutación por error inesperada, los recursos muestran "iniciado (en caso de fallo)" en el estado de los pc cuando se activa la delimitación

Problema probable: se produjo Un problema que provocó una conmutación por error, pero Pacemaker no pudo verificar que el nodo estaba vallado. Esto podría ocurrir porque la delimitación estaba mal configurada o hubo un problema con el agente de cercado (ejemplo: La PDU se desconectó de la red).

Cómo resolver:

1. Compruebe que el nodo esté apagado.



Si el nodo que especifique no está apagado pero si ejecuta servicios o recursos del clúster, se producirán errores en los datos o en el clúster.

2. Confirmar manualmente la esgrima con: `pcs stonith confirm <NODE>`

En este punto, los servicios deben terminar de conmutar por error y reiniciarse en otro nodo en buen estado.

Tareas comunes de solución de problemas

Reinic peace los servicios BeeGFS individuales

Normalmente, si es necesario reiniciar un servicio BeeGFS (por ejemplo, para facilitar un cambio en la configuración), debe hacerlo actualizando el inventario de Ansible y volviendo a ejecutar el libro de estrategia. En algunos casos, puede que sea conveniente reiniciar servicios individuales para facilitar la solución de problemas más rápida, por ejemplo, cambiar el nivel de registro sin tener que esperar a que se ejecute el libro de estrategia completo.



A menos que también se añadan cambios manuales al inventario de Ansible, se revertirá la próxima vez que se ejecute el libro de estrategia de Ansible.

Opción 1: Reinicio controlado por sistema

Si existe un riesgo de que el servicio BeeGFS no se reinicie correctamente con la nueva configuración, coloque primero el clúster en modo de mantenimiento para evitar que el monitor BeeGFS detecte que el servicio se detiene y active una conmutación por error no deseada:

```
pcs property set maintenance-mode=true
```

Si es necesario, realice cualquier cambio en la configuración de servicios en `/mnt/<SERVICE_ID>/__config/beegfs-.conf` (ejemplo: `/mnt/meta_01_tgt_0101/metadata_config/beegfs-meta.conf`) a continuación, utilice systemctl para reiniciarlo:

```
systemctl restart beegfs-*@<SERVICE_ID>.service
```

Ejemplo: `systemctl restart beegfs-meta@meta_01_tgt_0101.service`

Opción 2: Reinicio controlado por marcapasos

Si no le preocupa la nueva configuración, puede hacer que el servicio se detenga de forma inesperada (por ejemplo, simplemente cambiando el nivel de registro), o está en una ventana de mantenimiento y no le preocupa el tiempo de inactividad, puede reiniciar el monitor BeeGFS para el servicio que desea reiniciar:

```
pcs resource restart <SERVICE>-monitor
```

Por ejemplo, para reiniciar el servicio de gestión de BeeGFS: pcs resource restart mgmt-monitor

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.