RED HAT CUSTOMER PORTAL

Red Hat Enterprise Linux 6

Administración de clúster

Cómo configurar y administrar adiciones de alta disponibilidad

Edición 0

Aviso Legal

1801 Varsity Drive
Raleigh, NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701

Resumen

Cómo configurar y administrar adiciones de alta disponibilidad describe la configuración y administración de adiciones de alta disponibilidad para Red Hat Enterprise Linux 6.

Introducción
1. Convenciones del Documento
1.1. Convenciones tipográficas
1.2. Convenciones del documento

1.3. Notas y Advertencias

2. Comentarios

1. Configuración de adición de alta disponibilidad y visión general de administración de Red Hat
1.1. Funcionalidades nuevas y cambiadas
1.1.1. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.1
1.1.2. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.2
1.1.3. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.3
1.1.4. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.4
1.2. Fundamentos de configuración
1.3. Cómo configurar hardware
1.4. Cómo instalar adición de software de Alta disponibilidad de Red Hat
1.5. Configuración de software de adición de Alta disponibilidad de Red Hat

2. Antes de configurar la adición de alta disponibilidad de Red Hat
2.1. Consideraciones generales de configuración
2.2. Hardware compatible
2.3. Cómo habilitar puertos IP
2.3.1. Cómo habilitar puertos IP en nodos de clúster
2.3.2. Activación del puerto IP para luci
2.3.3. Cómo configurar el cortafuegos de iptables para permitir componentes de clúster
2.4. Configuración de luci con `/etc/sysconfig/luci`
2.5. Cómo configurar ACPI para usar con dispositivos de valla integrados
2.5.1. Desactivar ACPI Soft-Off con administración de `chkconfig`
2.5.2. Desactivar ACPI Soft-Off con el BIOS
2.5.3. Desactivar completamente a ACPI en el archivo `grub.conf`
2.6. Consideraciones para configurar servicios de alta disponibilidad
2.7. Validación de configuración
2.8. Consideraciones para NetworkManager
2.9. Consideraciones para usar disco de cuórum
2.10. Adición de alta disponibilidad de Red Hat y SELinux
2.11. Direcciones de multidifusión
2.12. Tráfico unidifusión UDP
2.13. Consideraciones para `ricci`
2.14. Configuración de las máquinas virtuales en un entorno en clúster.

3. Configuración de adición de alta disponibilidad de Red Hat con Conga
3.1. Tareas de configuración
3.2. Inicio de luci
3.3. Cómo controlar el acceso a luci
3.4. Cómo crear un clúster
3.5. Propiedades globales de clúster
3.5.1. Propiedades generales de configuración
3.5.2. Configuración de propiedades de demonio de valla
3.5.3. Configuración de red
3.5.4. Cómo configura el protocolo de anillos redundantes
3.5.5. Configuración de disco de cuórum
3.5.6. Configuración de registro
3.6. Configuración de dispositivos de valla
3.6.1. Cómo crear un dispositivo de valla
3.6.2. Modificación de un dispositivo de valla
3.6.3. Borrado de un dispositivo de valla
3.7. Configuración de cercado para miembros de clúster
3.7.1. Configuración de un dispositivo de vallas único para un nodo
3.7.2. Configuración de un dispositivo de vallas de respaldo
3.7.3. Configuración de un nodo con energía redundante
3.8. Configuración de dominio de conmutación
3.8.1. Adición de un dominio de conmutación
3.8.2. Modificación de un dominio de conmutación
3.8.3. Borrado de un dominio de conmutación
3.9. Configuración de recursos de clúster globales
3.10. Adición de un servicio de clúster al clúster

4. Administración de adición de alta disponibilidad de Red Hat con Conga
4.1. Añadir un clúster existente a la interfaz luci
4.2. Retirar un clúster existente a la interfaz luci
4.3. Administrar nodos de clúster

4.3.1. Reinicio de un nodo de clúster
4.3.2. Hacer que un nodo abandone o se una a un clúster
4.3.3. Añadir un miembro a un clúster en ejecución
4.3.4. Borrado de un miembro de un clúster

4.4. Iniciar, parar, reiniciar, y borrar clústeres
4.5. Administrar servicios de alta disponibilidad
4.6. Cómo hacer una copia de seguridad y restaurar la configuración de luci

5. Configuración de adición de alta disponibilidad de Red Hat con el comando ccs
5.1. Visión general operativa
5.1.1. Cómo crear un archivo de configuración de clúster en un sistema local
5.1.2. Cómo ver la configuración de clúster actual
5.1.3. Cómo especificar contraseñas ricci con el comando ccs
5.1.4. Cómo modificar componentes de configuración de clúster
5.1.5. Comandos que sobrescriben los parámetros anteriores
5.1.6. Validación de configuración

5.2. Tareas de configuración
5.3. Cómo iniciar ricci
5.4. Cómo crear un clúster
5.5. Cómo configurar dispositivos de valla
5.6. Cómo listar dispositivos de vallas y opciones de dispositivos de vallas
5.7. Cómo configurar cercado para miembros de clúster
5.7.1. Cómo configurar un dispositivo de valla basado en energía simple para un nodo
5.7.2. Cómo configurar un dispositivo de valla basado en almacenamiento simple para un nodo
5.7.3. Cómo configurar un dispositivo de valla de respaldo
5.7.4. Cómo configurar un nodo con energía redundante
5.7.5. Cómo retirar métodos de valla e instancias de valla

5.8. Cómo configurar un dominio de conmutación
5.9. Cómo configurar recursos de clúster global
5.10. Adición de un servicio de clúster al clúster
5.11. Listado de cluster disponibles
5.12. Recursos de máquinas virtuales
5.13. Cómo configurar un disco de cuórum
5.14. Varios de configuración de clúster
5.14.1. Versión de configuración de clúster
5.14.2. Configuración de multidifusión
5.14.3. Cómo configurar un clúster de dos nodos
5.14.4. Registro
5.14.5. Cómo configurar el protocolo de anillo redundante

5.15. Cómo propagar el archivo de configuración a los nodos de clúster

6. Administración de adición de alta disponibilidad de Red Hat con ccs
6.1. Administrar nodos de clúster
6.1.1. Hacer que un nodo abandone o se una a un clúster
6.1.2. Añadir un miembro a un clúster en ejecución

6.2. Cómo iniciar y detener un clúster
6.3. Cómo diagnosticar y corregir problemas en un clúster

7. Configuración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos
7.1. Tareas de configuración
7.2. Creación de un archivo de configuración de clúster básico
7.3. Configuración de vallas
7.4. Configuración de dominios de conmutación
7.5. Configuración de servicios de alta disponibilidad
7.5.1. Adición de recursos de clúster
7.5.2. Adición de un servicio de clúster al clúster

7.6. Cómo configura el protocolo de anillos redundantes
7.7. Configuración de opciones de depuración
7.8. Verificación de una configuración

8. Administración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos
8.1. Iniciar y parar el software de clúster
8.1.1. Cómo iniciar software de clúster
8.1.2. Cómo detener el software de clúster

8.2. Borrar o añadir un nodo

8.2.1. Cómo borrar un nodo de un clúster
8.2.2. Adición de un nodo a un cluster
8.2.3. Ejemplos de configuraciones de tres y dos nodos.

8.3. Administrar servicios de alta disponibilidad
8.3.1. Cómo desplegar el estatus de servicio de alta disponibilidad con `clustat`
8.3.2. Cómo administrar servicios de alta disponibilidad con `clusvcadm`

8.4. Cómo actualizar una configuración
8.4.1. Cómo actualizar una configuración con `cman_tool version -r`
8.4.2. Actualizar y configurar mediante `scp`

9. Cómo diagnosticar y corregir problemas en un clúster
9.1. Los cambios de configuración no se efectúan
9.2. El clúster no se forma
9.3. Nodos que no pueden reconectar clúster tras un cercado o reinicio
9.4. El demonio de clúster se bloquea
9.4.1. Captura del núcleo `rgmanager` en tiempo de ejecución
9.4.2. Captura del núcleo cuando el demonio se bloquea
9.4.3. Registro de una sesión `gdb` de seguimiento

9.5. Colgado de servicios de clúster
9.6. El servicio de clúster no iniciará
9.7. Servicio controlado de clúster falla al migrar
9.8. Cada nodo en un reporte de clúster de dos nodos reporta el segundo nodo caído
9.9. Nodos se cercan en Falla de ruta LUN
9.10. El disco de cuórum no aparece como miembro de clúster
9.11. Conducta de conmutación inusual
9.12. El cercado se presenta en forma aleatoria
9.13. El registro de depuración para el Gestor de bloqueo distribuido (DLM) necesita estar habilitado.

10. Configuración de SNMP con adición de alta disponibilidad de Red Hat
10.1. SNMP y adición de alta disponibilidad de Red Hat
10.2. Configuración SNMP con la adición de alta disponibilidad de Red Hat
10.3. Cómo reenviar capturas SNMP
10.4. Capturas SNMP producidas por la adición de alta disponibilidad de Red Hat

11. Configuraciones de Samba en clúster
11.1. Visión general de CTDB
11.2. Paquetes requeridos
11.3. Configuración de GFS2
11.4. Configuración de CTDB
11.5. Configuración de Samba
11.6. Cómo iniciar CTDB y los servicios de Samba
11.7. Cómo usar el servidor Samba en clúster

A. Parámetros de dispositivos de valla

B. Parámetros de recursos de alta disponibilidad

C. Comportamiento de recursos de alta disponibilidad
C.1. Relaciones padre, hijo y hermanos entre recursos
C.2. Solicitud de inicio para hermanos y solicitud de hijo de recursos
C.2.1. Solicitud de inicio y parada de recursos de hijo tipificado
C.2.2. Solicitud de inicio y parada de los recursos de hijo no-tipificado

C.3. Herencia, los "recursos" Bloques y reutilización de recursos
C.4. Recuperación de fallas y subárboles independientes
C.5. Depuración y prueba de servicios y ordenamiento de recursos

D. Revisión de recursos de servicios de clúster y tiempo de espera de conmutación
D.1. Cómo modificar el intervalo de revisión de estatus de recursos
D.2. Aplicación de tiempos de espera en recursos

E. Resumen de herramientas de línea de comandos

F. Alta disponibilidad de LVM (HA-LVM)
F.1. Configuración de conmutación de HA-LVM con CLVM (preferido)
F.2. Configuración de conmutación HA-LVM con etiquetas

G. Historial de revisiones

Índice

Introducción

Este documento proporciona información sobre instalación, configuración y administración de componentes de adiciones de alta disponibilidad de Red Hat. Los componentes de adiciones de alta disponibilidad de Red Hat le permiten conectar a un grupo de computadores (llamados *nodos* o *miembros*) para que funcionen juntos como un clúster. En este documento, el uso de la palabra *clúster* o *clúster* se utiliza para referirse a un grupo de computadores que ejecutan la adición de alta disponibilidad de Red Hat.

La audiencia de este documento debe tener amplia experiencia con Red Hat Enterprise Linux y comprender los conceptos de clúster, almacenamiento y servidor de informática.

Para obtener mayor información acerca de Red Hat Enterprise Linux 6, consulte los siguientes recursos:

- *Guía de instalación de Red Hat Enterprise Linux* — Proporciona información sobre instalación de Red Hat Enterprise Linux 6.
- *Guía de implementación de Red Hat Enterprise Linux* — Proporciona información sobre la implementación, configuración y administración de Red Hat Enterprise Linux 6.

Para obtener mayor información sobre la adición de alta disponibilidad y productos relacionados para Red Hat Enterprise Linux 6, consulte los siguientes recursos:

- *Visión general de adicón de alta disponibilidad* — Proporciona una descripción general de la adición de alta disponibilidad de Red Hat.
- *Gestión del administrador de volúmenes lógicos* — Proporciona una descripción del Administrador de volúmenes lógicos (LVM), incluyendo información sobre LVM en ejecución en un entorno de clúster.
- *Sistemas de archivos global 2: Configuración y administración* — Proporciona información sobre instalación, configuración, y mantenimiento de Red Hat GFS2 (Red Hat Global File System 2), el cual está incluido en la adición del almacenamiento resistente.
- *DM Multirutas* — Proporciona información sobre la función del dispositivo mapeador multirutas de Red Hat Enterprise Linux 6.
- *Administración de equilibrador de cargas* — Proporciona información sobre configuración de sistemas y servicios de alto rendimiento con la adición del equilibrador de cargas de Red Hat, un conjunto de componentes de software integrados que proporcionan Servidores virtuales de Linux (LVS) para equilibrar cargas IP a través de un conjunto de servidores reales.
- *Notas de lanzamiento* — Proporciona información sobre el lanzamiento actual de productos de Red Hat.

La documentación de adición de alta disponibilidad y otros documentos de Red Hat están disponibles en versiones HTML, PDF, y RPM en el CD de documentación de Red Hat Enterprise Linux y en línea en http://docs.redhat.com/docs/en-US/index.html.

1. Convenciones del Documento

Este manual utiliza varias convenciones para resaltar algunas palabras y frases y llamar la atención sobre ciertas partes específicas de información.

En ediciones PDF y de papel, este manual utiliza tipos de letra procedentes de Liberation Fonts. Liberation Fonts también se utilizan en ediciones de HTML si están instalados en su sistema. Si no, se muestran tipografías alternativas pero equivalentes. Nota: Red Hat Enterprise Linux 5 y siguientes incluyen Liberation Fonts predeterminadas.

1.1. Convenciones tipográficas

Se utilizan cuatro convenciones tipográficas para llamar la atención sobre palabras o frases específicas. Dichas convenciones y las circunstancias en que se aplican son las siguientes:

`Negrita monoespaciado`

Utilizado para resaltar la entrada del sistema, incluyendo los comandos de shell, nombres de archivos y rutas. También sirve para resaltar teclas y combinaciones de teclas. Por ejemplo:

> Para ver el contenido del archivo **`my_next_bestselling_novel`** en su directorio actual de trabajo, escriba el comando **`cat my_next_bestselling_novel`** en el intérprete de comandos de shell y pulse **`Enter`** para ejecutar el comando.

El ejemplo anterior incluye un nombre de archivo, un comando de shell y una tecla . Todo se presenta en negrita-monoespaciado y distinguible gracias al contexto.

Las combinaciones de teclas se pueden distinguir de las individuales con el signo más que conecta cada partee de la combinación de tecla. Por ejemplo:

> Pulse **Enter** para ejecutar el comando.
>
> Pulse **Ctrl+Alt+F2** para pasar a una terminal virtual.

El primer ejemplo resalta una tecla particular a pulsar. El segundo ejemplo, resalta una combinación de teclas: un set de tres teclas pulsadas simultáneamente.

Si se discute el código fuente, los nombres de las clase, los métodos, las funciones, los nombres de variables y valores de retorno mencionados dentro de un párrafo serán presentados en **Negrita-monoespaciado**. Por ejemplo:

> Las clases de archivo relacionadas incluyen **filename** para sistema de archivos, **file** para archivos y **dir** para directorios. Cada clase tiene su propio conjunto asociado de permisos.

Negrita proporcional

Esta denota palabras o frases encontradas en un sistema, incluyendo nombres de aplicación, texto de cuadro de diálogo, botones etiquetados, etiquetas de cajilla de verificación y botón de radio; títulos de menú y títulos del submenú. Por ejemplo:

> Seleccionar **Sistema** → **Preferencias** → **Ratón** desde la barra del menú principal para lanzar **Preferencias de Ratón**. En la pestaña de **Botones**, haga clic en la cajilla **ratón de mano izquierda** y luego haga clic en **Cerrar** para cambiar el botón principal del ratón de la izquierda a la derecha (adecuando el ratón para la mano izquierda).
>
> Para insertar un carácter especial en un archivo **gedit**, seleccione **Aplicaciones** → **Accesorios** → **Mapa de caracteres** de la barra del menú. Luego, seleccione **Búsqueda** → **Buscar…** de la barra del menú de **Mapa de caracteres**, escriba el nombre del carácter en el campo de **Búsqueda** y haga clic en **Siguiente**. El carácter que buscó será resaltado en la **Tabla de caracteres**. Haga doble clic en ese carácter resaltado para colocarlo en el campo de **Texto a copiar** y luego haga clic en el botón **Copiar**. Ahora regrese al documento y elija **Modificar** → **Pegar** de la barra de menú de **gedit**.

El texto anterior incluye nombres de aplicación; nombres y elementos del menú de todo el sistema; nombres de menú de aplicaciones específicas y botones y texto hallados dentro de una interfaz gráfica de usuario, todos presentados en negrita proporcional y distinguibles por contexto.

Itálicas-negrita monoespaciado o ***Itálicas-negrita proporcional***

Ya sea negrita monoespaciado o negrita proporcional, la adición de itálicas indica texto reemplazable o variable. Las itálicas denotan texto que usted no escribe literalmente o texto mostrado que cambia dependiendo de la circunstancia. Por ejemplo:

> Para conectar a una máquina remota utilizando ssh, teclee **ssh *nombre de usuario*@*dominio.nombre*** en un intérprete de comandos de shell. Si la máquina remota es **example.com** y su nombre de usuario en esa máquina es john, teclee **ssh john@example.com**.
>
> El comando **mount -o remount *file-system*** remonta el sistema de archivo llamado. Por ejemplo, para volver a montar el sistema de archivo **/home**, el comando es **mount -o remount /home**.
>
> Para ver la versión de un paquete actualmente instalado, utilice el comando **rpm -q *paquete***. Éste entregará el resultado siguiente: ***paquete-versión-lanzamiento***.

Observe que las palabras resaltadas en itálicas — nombre de usuario, dominio.nombre, sistema de archivo, paquete, versión y lanzamiento. Cada palabra es un marcador de posición, ya sea de texto a ingresar cuando se ejecuta un comando o para un texto ejecutado por el sistema.

Aparte del uso estándar para presentar el título de un trabajo, las itálicas denotan el primer uso de un término nuevo e importante. Por ejemplo:

> Publican es un sistema de publicación de *DocBook*.

1.2. Convenciones del documento

Los mensajes de salida de la terminal o fragmentos de código fuente se distinguen visualmente del texto circundante.

Los mensajes de salida enviados a una terminal se muestran en **romano monoespaciado** y se presentan así:

```
books        Desktop   documentation  drafts  mss    photos   stuff  svn
books_tests  Desktop1  downloads      images  notes  scripts  svgs
```

Los listados de código fuente también se muestran en **romano monoespaciado**, pero se presentan y resaltan de la siguiente manera:

```
package org.jboss.book.jca.ex1;

import javax.naming.InitialContext;

public class ExClient
{
   public static void main(String args[])
       throws Exception
   {
      InitialContext iniCtx = new InitialContext();
      Object         ref    = iniCtx.lookup("EchoBean");
      EchoHome       home   = (EchoHome) ref;
      Echo           echo   = home.create();

      System.out.println("Created Echo");

      System.out.println("Echo.echo('Hello') = " + echo.echo("Hello"));
   }
}
```

1.3. Notas y Advertencias

Finalmente, utilizamos tres estilos visuales para llamar la atención sobre la información que de otro modo se podría pasar por alto.

Nota

Una nota es una sugerencia, atajo o enfoque alternativo para una tarea determinada. Ignorar una nota no debería tener consecuencias negativas, pero podría perderse de algunos trucos que pueden facilitarle las cosas.

Importante

Los cuadros con el título de importante dan detalles de cosas que se pueden pasar por alto fácilmente: cambios de configuración únicamente aplicables a la sesión actual, o servicios que necesitan reiniciarse antes de que se aplique una actualización. Ignorar estos cuadros no ocasionará pérdida de datos, pero puede causar enfado y frustración.

Aviso

Las advertencias no deben ignorarse. Ignorarlas muy probablemente ocasionará pérdida de datos.

2. Comentarios

Si encuentra un error tipográfico o si ha pensado en alguna forma de mejorar este manual, nos encantaría saberlo. Por favor, envíe un informe en Bugzilla (http://bugzilla.redhat.com/bugzilla/) con el componente **doc-Cluster_Administration**.

Asegúrese de mencionar el identificador del manual:

```
Cluster_Administration(EN)-6 (2013-2-15T16:26)
```

Al mencionar este identificador de manual, sabemos exactamente qué versión de la guía tiene usted.

Si tiene alguna sugerencia de cómo mejorar la documentación, por favor trate de ser lo más

explícito posible. Si ha encontrado algún error, incluya el número de la sección y parte del texto que lo rodea para así poderlo hallar fácilmente.

Capítulo 1. Configuración de adición de alta disponibilidad y visión general de administración de Red Hat

1.1. Funcionalidades nuevas y cambiadas
1.1.1. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.1
1.1.2. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.2
1.1.3. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.3
1.1.4. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.4

1.2. Fundamentos de configuración

1.3. Cómo configurar hardware

1.4. Cómo instalar adición de software de Alta disponibilidad de Red Hat

1.5. Configuración de software de adición de Alta disponibilidad de Red Hat

La adición de alta disponibilidad de Red Hat permite la conexión al grupo de computadores (llamado *nodos* o *miembros*) para funcionar juntos como un clúster. Puede utilizar la adición de alta disponibilidad de Red Hat para que se ajuste a sus necesidades de agrupamiento (Por ejemplo, configurar un clúster para compartir archivos en un archivo GFS2 o configurar un servicio de conmutación).

Nota

Para obtener información sobre las mejores prácticas para implementar y actualizar los clústeres de Red Hat Enterprise Linux mediante la adición de alta disponibilidad y el Sistema de archivos globales 2 de Red Hat (GFS2), consulte el artículo "Red Hat Enterprise Linux Cluster, High Availability, y GFS Deployment Best Practices" en Red Hat Customer Portal, . https://access.redhat.com/kb/docs/DOC-40821.

Este capítulo provee un resumen de funcionalidades de documentación y actualizaciones que han sido añadidas a la adición de alta disponibilidad de Red Hat desde el lanzamiento inicial de Red Hat Enterprise Linux 6, seguido por una visión general de configuración y manejo de adición de alta disponibilidad de Red Hat.

1.1. Funcionalidades nuevas y cambiadas

Esta sección lista las funcionalidades nuevas y cambiadas de la documentación de adición de alta disponibilidad que ha sido añadida desde el lanzamiento inicial de Red Hat Enterprise Linux 6.

1.1.1. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.1

Red Hat Enterprise Linux 6.1 incluye la siguiente documentación y actualizaciones y cambios de funcionalidades.

- A partir del lanzamiento de Red Hat Enterprise Linux 6.1, la adición de alta disponibilidad de Red Hat proporciona soporte para capturas SNMP. Para información sobre configuración de capturas SNMP con la adición de alta disponibilidad de Red Hat, consulte el Capítulo 10, *Configuración de SNMP con adición de alta disponibilidad de Red Hat*.
- A partir del lanzamiento de Red Hat Enterprise Linux 6.1, la adición de alta disponibilidad de Red Hat provee el soporte para el comando de configuración de clúster **ccs**. Para obtener mayor información sobre el comando **ccs**, consulte el Capítulo 5, *Configuración de adición de alta disponibilidad de Red Hat con el comando* ***ccs*** y el Capítulo 6, *Administración de adición de alta disponibilidad de Red Hat con* ***ccs***.
- La documentación de configuración y manejo de adición de Alta disponibilidad de Red Hat mediante Conga ha sido actualizado para reflejar las pantallas de de Conga actualizadas y el soporte de funcionalidades.
- Para el lanzamiento de Red Hat Enterprise Linux 6.1 y posterior, el uso de **ricci** requiere una contraseña la primera vez que usted propaga la configuración de clúster desde un nodo determinado. Para obtener información sobre **ricci**, consulte la Sección 2.13, “Consideraciones para **ricci**”.
- Puede especificar una política de falla de *Restart-Disable* para un servicio, indicando que el sistema debe intentar reiniciar el servicio en el sitio si se produce un error, pero si al reiniciar el servicio falla, el servicio se inhabilitará en lugar de ser desplazado a otro host en el clúster. Esta funcionalidad se documenta en la Sección 3.10, “Adición de un servicio de clúster al clúster” y en el Apéndice B, *Parámetros de recursos de alta disponibilidad*.

- Ahora puede configurar un subárbol independiente como no-crítico, indicando que si el recurso falla, entonces solo ese recurso se inhabilitará. Para obtener información sobre esta funcionalidad, consulte la Sección 3.10, “Adición de un servicio de clúster al clúster” y la Sección C.4, “Recuperación de fallas y subárboles independientes”.
- Este documento ahora incluye el nuevo capítulo Capítulo 9, *Cómo diagnosticar y corregir problemas en un clúster*.

Además, se han hecho correcciones y aclaraciones a lo largo del documento.

1.1.2. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.2

Red Hat Enterprise Linux 6.2 incluye la siguiente documentación y presenta actualizaciones y cambios.

- Red Hat Enterprise Linux ahora proporciona soporte para ejecutar Samba en clúster en una configuración activa/activa. Para obtener información sobre configuración de Samba en clúster, consulte el Capítulo 11, *Configuraciones de Samba en clúster*.
- Aunque cualquier usuario capaz de autenticarse en el sistema que alberga **luci** puede ingresar a **luci**, a partir del lanzamiento de Red Hat Enterprise Linux 6.2 solo el usuario root en el sistema que esté ejecutando **luci** puede acceder a cualquiera de los componentes de **luci** hasta que un administrador (el usuario root u otro usuario con permisos de administrador) establezca los permisos para ese usuario. Para obtener información sobre cómo establecer permisos de **luci** para usuarios, consulte la Sección 3.3, “Cómo controlar el acceso a luci”.
- Los nodos en un clúster se pueden comunicar entre sí mediante el mecanismo de transporte unidifusión UDP. Para obtener información sobre cómo configurar unidifusión UDP, consulte la Sección 2.12, “Tráfico unidifusión UDP”.
- Puede configurar algunos aspectos de la conducta de **luci** mediante el archivo **/etc/sysconfig/luci**. Por ejemplo, puede específicamente configurar la única dirección IP en la que **luci** se sirve. Para obtener información sobre configuración de la única dirección IP en la que **luci** se sirve, consulte la Tabla 2.2, “Puertos IP habilitados en un computador que ejecuta luci”. Para obtener información sobre el archivo **/etc/sysconfig/luci** en general, consulte la Sección 2.4, “Configuración de **luci** con **/etc/sysconfig/luci**”.
- Ahora, el comando **ccs** incluye la opción **--lsfenceopts**, la cual escribe en pantalla una lista de los dispositivos de valla disponibles, y la opción **--lsfenceopts *fence_type*** que imprime cada tipo de valla disponible. Para obtener información sobre estas opciones, consulte la Sección 5.6, “Cómo listar dispositivos de vallas y opciones de dispositivos de vallas ”.
- Ahora el comando **ccs** incluye la opción **--lsserviceopts** que imprime en pantala una lista de los servicios de clúster actualmente disponibles para su clúster y la opción **--lsserviceopts *service_type***, la cual imprime una lista de las opciones que puede especificar para un tipo de servicion particular. Para obtener información sobre dichas opciones, consulte la Sección 5.11, “Listado de cluster disponibles ”.
- El lanzamiento de Red Hat Enterprise Linux 6.2 provee soporte para el agente de valla de VMware (Interfaz SOAP). Para obtener información sobre los parámetros de dispositivos de vallas, consulte el Apéndice A, *Parámetros de dispositivos de valla*.
- El lanzamiento de Red Hat Enterprise Linux 6.2 provee soporte para el agente de valla de RHEV-M REST API, con RHEV 3.0 y posterior. Para obtener información sobre parámetros de dispositivos, consulte el Apéndice A, *Parámetros de dispositivos de valla*.
- A partir de Red Hat Enterprise Linux 6.2 release, usted configura la máquina virtual en un clúster con el comando **ccs** usted puede usar la opción **--addvm** (en lugar de la opción **addservice**). Así garantiza que el recurso de **vm** se defina directamente bajo el nodo de configuración **rm** en el archivo de configuración de clúster. Para obtener información sobre recursos de máquina virtual con el comando **ccs** consulte la Sección 5.12, “Recursos de máquinas virtuales”.
- Este documento incluye el nuevo apéndice Apéndice D, *Revisión de recursos de servicios de clúster y tiempo de espera de conmutación*, el cual describe cómo **rgmanager** monitoriza el estatus de recursos de clúster y cómo modificar el intervalo de revisión de estatus. El apéndice también describe el parámetro de servicio **__enforce_timeouts**, el cual indica que un tiempo de espera para una operación puede hacer que un servicio falle.
- Este documento incluye una nueva sección, la Sección 2.3.3, “Cómo configurar el cortafuegos de iptables para permitir componentes de clúster”. Esta sección muestra el filtraje que puede utilizar para permitir el tráfico multidifusión a través del cortafuegos **iptables** para varios componentes de clúster.

Además, se han hecho correcciones y aclaraciones a lo largo del documento.

1.1.3. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.3

Red Hat Enterprise Linux 6.3 incluye la siguiente documentación y presenta actualizaciones y cambios.

- El lanzamiento de Red Hat Enterprise Linux 6.3 provee soporte par el agente de recursos **condor**. Para obtener información sobre los parámetros de recursos de alta disponibilidad, consulte el Apéndice B, *Parámetros de recursos de alta disponibilidad*.
- Este documento ahora incluye un nuevo apéndice, Apéndice F, *Alta disponibilidad de LVM (HA-LVM)*.
- La información a través de este documento aclara los cambios de configuración requeridos para reiniciar un clúster. Para obtener un resumen de dichos cambios, consulte la Sección 9.1, "Los cambios de configuración no se efectúan".
- la documentación ahora anota que hay un tiempo de espera inactivo para **luci** que lo saca después de 15 minutos de inactividad. Para obtener mayor información sobre cómo iniciar a **luci**, consulte la Sección 3.2, "Inicio de **luci**".
- El dispositivo de valla **fence_ipmilan** soporta un parámetro de nivel de privilegio. Para obtener información sobre parámetros de dispositivos de valla, consulte el Apéndice A, *Parámetros de dispositivos de valla*.
- Este documento ahora incluye una nueva sección, la Sección 2.14, "Configuración de las máquinas virtuales en un entorno en clúster.".
- Este documento ahora incluye una nueva sección, la Sección 4.6, "Cómo hacer una copia de seguridad y restaurar la configuración de luci".
- Este documento ahora incluye una nueva sección, laSección 9.4, "El demonio de clúster se bloquea".
- Este documento provee información sobre cómo configurar la opción de depuración en las secciones Sección 5.14.4, "Registro", Sección 7.7, "Configuración de opciones de depuración" y Sección 9.13, "El registro de depuración para el Gestor de bloqueo distribuido (DLM) necesita estar habilitado.".
- A partir de Red Hat Enterprise Linux 6.3, el usuario root o aquel a quien se le han otorgado permisos administrativos de **luci** también puede usar la interfaz de **luci** para añadir usuarios al sistema, así como se describe en la Sección 3.3, "Cómo controlar el acceso a luci".
- A partir de Red Hat Enterprise Linux 6.3, el comando **ccs** valida la configuración según el esquema de clúster en **/usr/share/cluster/cluster.rng** en el nodo que especifica con la opción **-h**. Anteriormente el comando **ccs** siempre utilizaba el esquema de clúster que era empaquetado con el propio comando **ccs** command itself, **/usr/share/ccs/cluster.rng** en el sistema local. Para obtener información sobre validación de configuración, consulte la Sección 5.1.6, "Validación de configuración".
- Las tablas que describen los parámetros de dispositivos de valla en el Apéndice A, *Parámetros de dispositivos de valla* y las que describen los recursos de alta disponibilidad en el Apéndice B, *Parámetros de recursos de alta disponibilidad*, ahora incluyen los nombres de los parámetros como aparecen en el archivo **cluster.conf**.

Además, se han hecho correcciones y aclaraciones a lo largo del documento.

1.1.4. Funcionalidades nuevas y cambiadas para Red Hat Enterprise Linux 6.4

Red Hat Enterprise Linux 6.4 incluye la siguiente documentación y presenta actualizaciones y cambios.

- El lanzamiento de Red Hat Enterprise Linux 6.4 provee soporte para el agente de valla del Controlador de energía de red Eaton, (interfaz SNMP), el agente HP Bladesystem y el agente de vallas IBM IPDU. Para obtener mayor información sobre los parámetros de dispositivos de valla, consulte el Apéndice A, *Parámetros de dispositivos de valla*.
- Ahora Apéndice B, *Parámetros de recursos de alta disponibilidad* proporciona una descripción del agente de recursos de servidor NFS.
- A partir de Red Hat Enterprise Linux 6.4, el usuario root o aquel a quien se le han otorgado permisos administrativos de **luci** también puede usar la interfaz de **luci** para borrar usuarios del sistema, así como se describe en la Sección 3.3, "Cómo controlar el acceso a luci".
- El Apéndice B, *Parámetros de recursos de alta disponibilidad* proporciona una descripción del nuevo parámetro **nfsrestart** para el sistema de archivos y los recursos de alta disponibilidad GFS2.
- Este documento incluye una nueva sección, la Sección 5.1.5, "Comandos que sobrescriben los parámetros anteriores".
- La Sección 2.3, "Cómo habilitar puertos IP" ahora incluye información sobre filtraje del cortafuegos de **iptables** para **igmp**.

- El agente de valla IPMI LAN soporta un parámetro para configurar el nivel de privilegios sobre el dispositivo IPMI, como se documenta en el Apéndice A, *Parámetros de dispositivos de valla*.
- Aparte del modo de enlace 1 Ethernet, los modos de enlace 0 y 2 ahora tienen soporte para comunicación internodos en un clúster. El aviso de Detección y corrección de errores en este documento,que sugiere verificar si se están utilizando únicamente modos de enlace, ahora toma nota de esto.
- Los dispositivos etiquetados de VLAN ahora tienen soporte para comunicación de clúster heartbeat. El aviso de Detección y corrección de errores que indicaba que no tenían soporte, ha sido retirado de este documento.
- La adición de alta disponibilidad de Red Hat ahora soporta la configuración de protocolo de anillos redundantes. Para obtener información general sobre el uso de esta funcionalidad y de la configuración del archivo de configuración `cluster.conf`, consulte la Sección 7.6, "Cómo configura el protocolo de anillos redundantes". Para obtener información sobre protocolo de anillos redundantes con **luci**, consulte la Sección 3.5.4, "Cómo configura el protocolo de anillos redundantes". Para obtener información sobre cómo configurar protocolo de anillos redundantes con el comando `ccs`, consulte la Sección 5.14.5, "Cómo configurar el protocolo de anillo redundante".

Además, se han hecho correcciones y aclaraciones a lo largo del documento.

1.2. Fundamentos de configuración

Para configurar un clúster, debe conectar los nodos a algún hardware de clúster y configurar los nodos en el entorno de clúster. La configuración y administración de adición de alta disponibilidad de Red Hat consta de los siguientes pasos:

1. Configuración de hardware. Consulte la Sección 1.3, "Cómo configurar hardware".
2. Instalación y software de adición de alta disponibilidad Red Hat. Consulte la Sección 1.4, "Cómo instalar adición de software de Alta disponibilidad de Red Hat".
3. Configuración de adición de software de alta disponibilidad de Red Hat. Consulte la Sección 1.5, "Configuración de software de adición de Alta disponibilidad de Red Hat".

1.3. Cómo configurar hardware

La configuración de hardware consiste en conectar nodos de clúster a otro hardware requerido para ejecutar la adición de alta disponibilidad de Red Hat. La cantidad y tipo de hardware varía según el propósito y requerimientos de disponibilidad del clúster. Típicamente, un clúster a nivel empresarial requiere el tipo de hardware que se lista a continuación, (vea la Figura 1.1, "Vista general de hardware de adición de Alta disponibilidad de Red Hat "). Para consideraciones sobre hardware y detalles sobre configuración de clúster, consulte el Capítulo 2, *Antes de configurar la adición de alta disponibilidad de Red Hat* o contacte a su representante autorizado de Red Hat.

- Nodos de clúster — Computadores que ahora pueden ejecutar el software de Red Hat Enterprise Linux 6 con al menos 1GB de RAM.
- Interruptor de Ethernet o concentrador para redes públicas — Requerido para acceso de clientes al clúster.
- Interruptor Ethernet o concentrador para redes privadas — Requerido para comunicación entre nodos de clúster y otro hardware de clúster, tal como interruptores de redes y de canal de fibra.
- Interruptores de redes — Se recomienda un interruptor de alimentación de redes para realizar el cercado en un clúster de nivel empresarial.
- Interruptor de canal de fibra — Un interruptor de canal de fibra proporciona acceso a almacenaje de canal de fibra. Otras opciones están disponibles para almacenaje según el tipo de interfaz de almacenaje; por ejemplo, iSCSI. Un interruptor de canal de fibra puede ser configurado para realizar vallas.
- Almacenaje — Algún tipo de almacenaje se requiere para un clúster. El tipo requerido depende del propósito del clúster.

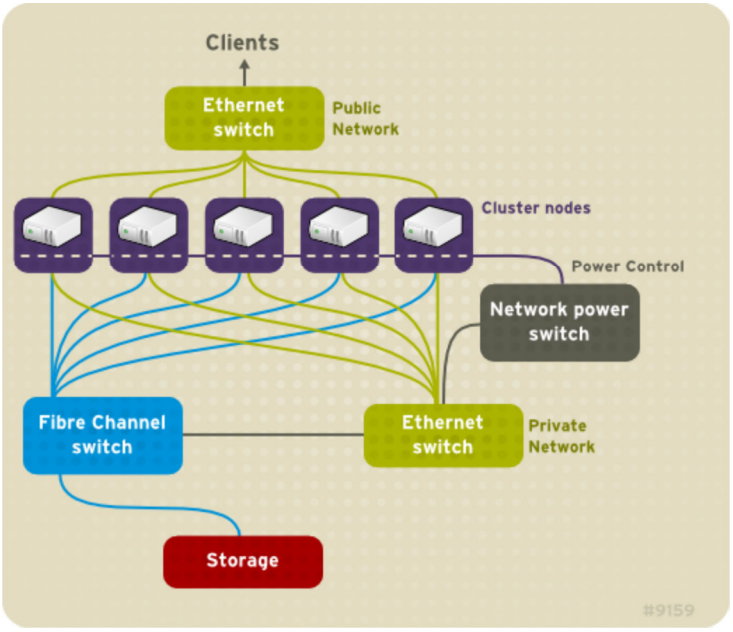

Figura 1.1. Vista general de hardware de adición de Alta disponibilidad de Red Hat

1.4. Cómo instalar adición de software de Alta disponibilidad de Red Hat

Para instalar la adición de alta disponibilidad de Red Hat, debe tener derechos para el software. Si está utilizando la Interfaz gráfica de usuario de configuración **luci**, puede permitirle instalar el software de clúster. Si está utilizando otras herramientas para configurar el clúster, asegure e instale el software como lo haría con el software de Red Hat Enterprise Linux.

Utilice el siguiente comando `yum install` para instalar los paquetes de software de alta disponibilidad de Red Hat:

```
# yum install rgmanager lvm2-cluster gfs2-utils
```

Observe que al instalar únicamente `rgmanager` extraerá todas las dependencias necesarias para crear un clúster de alta disponibilidad (HA) desde el canal de alta disponibilidad. Los paquetes `lvm2-cluster`y `gfs2-utils` son parte del canal ResilientStorage y pueden no necesitarse en su sitio.

Actualización de software de adición de Alta disponibilidad de Red Hat

Es posible actualizar el software de clúster en un lanzamiento mayor de Red Hat Enterprise Linux sin retirar el clúster de producción. Para hacer esto, debe desactivar el software de clúster en un host a la vez, actualiizando el software, y reiniciando el software de clúster en ese host.

1. Apague todos los servicios de clúster en un nodo de clúster único. Para obtener instrucciones sobre cómo detener software de clúster en un nodo, consulte la Sección 8.1.2, “Cómo detener el software de clúster”. Puede ser conveniente reubicar manualmente los servicios administrados de clúster y apagar las máquinas virtuales del host antes de detener `rgmanager`.
2. Ejecute el comando `yum update` para actualizar los paquetes instalados.
3. Rearranque el nodo de clúster o reinicie manualmente los servicios de clúster. Para obtener información sobre cómo iniciar software de clúster, consulte la Sección 8.1.1, “Cómo iniciar software de clúster”.

1.5. Configuración de software de adición de Alta disponibilidad de Red Hat

La configuración de software de adición de Alta disponibilidad de Red Hat consiste en usar herramientas de configuración para especificar la relación entre los componentes de clúster. Las siguientes herramientas de configuración de clúster están disponibles con adición de Alta disponibilidad de Red Hat:

- **Conga** — Esta es una interfaz de usuario global para instalar, configurar y administrar Red Hat adición de Alta disponibilidad. Consulte el Capítulo 3, *Configuración de adición de alta disponibilidad de Red Hat con **Conga*** y el Capítulo 4, *Administración de adición de alta disponibilidad de Red Hat con **Conga*** para obtener información acerca de cómo configurar y administrar la adición de Alta disponibilidad con **Conga**.
- El comando **ccs** — Este comando configura y administra adición de Alta disponibilidad de Red Hat. Consulte el Capítulo 5, *Configuración de adición de alta disponibilidad de Red Hat con el comando **ccs*** y el Capítulo 6, *Administración de adición de alta disponibilidad de Red Hat con **ccs*** para obtener información sobre configuración y administración de adición de Alta disponiblidad con el comando **ccs**.
- Herramientas de línea de comandos — Es un set de herramientas de línea de comandos para configurar y administrar la adición de Alta disponibilidad de Red Hat. Consulte el Capítulo 7, *Configuración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos* y el Capítulo 8, *Administración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos* para obtener información sobre configurar y administrar un clúster con herramientas de línea de comandos. Consulte el Apéndice E, *Resumen de herramientas de línea de comandos* para obtener un resumen de las herramientas de línea de comandos preferidas.

Nota

system-config-cluster no está disponible en Red Hat Enterprise Linux 6.

Capítulo 2. Antes de configurar la adición de alta disponibilidad de Red Hat

2.1. Consideraciones generales de configuración

2.2. Hardware compatible

2.3. Cómo habilitar puertos IP
- 2.3.1. Cómo habilitar puertos IP en nodos de clúster
- 2.3.2. Activación del puerto IP para luci
- 2.3.3. Cómo configurar el cortafuegos de iptables para permitir componentes de clúster

2.4. Configuración de luci con `/etc/sysconfig/luci`

2.5. Cómo configurar ACPI para usar con dispositivos de valla integrados
- 2.5.1. Desactivar ACPI Soft-Off con administración de `chkconfig`
- 2.5.2. Desactivar ACPI Soft-Off con el BIOS
- 2.5.3. Desactivar completamente a ACPI en el archivo `grub.conf`

2.6. Consideraciones para configurar servicios de alta disponibilidad

2.7. Validación de configuración

2.8. Consideraciones para NetworkManager

2.9. Consideraciones para usar disco de cuórum

2.10. Adición de alta disponibilidad de Red Hat y SELinux

2.11. Direcciones de multidifusión

2.12. Tráfico unidifusión UDP

2.13. Consideraciones para `ricci`

2.14. Configuración de las máquinas virtuales en un entorno en clúster.

Este capítulo describe las tareas a realizar y las consideraciones a tener antes de instalar y configurar la adición de alta disponibilidad de Red Hat. Consta de las siguientes secciones:

Importante

Asegúrese de que la implementación de la adición de alta disponibilidad de Red Hat satisfaga sus necesidades y pueda estar soportada. Consulte a un representante autorizado de Red Hat para verificar su configuración antes de implementarla. Además, disponga de un periodo de quemado de configuración para probar modos de fallas.

- Sección 2.1, “Consideraciones generales de configuración”
- Sección 2.2, “Hardware compatible”
- Sección 2.3, “Cómo habilitar puertos IP”
- Sección 2.4, “Configuración de **luci** con **`/etc/sysconfig/luci`**”
- Sección 2.5, “Cómo configurar ACPI para usar con dispositivos de valla integrados”
- Sección 2.6, “Consideraciones para configurar servicios de alta disponibilidad”
- Sección 2.7, “Validación de configuración”
- Sección 2.8, “Consideraciones para **NetworkManager**”
- Sección 2.9, “Consideraciones para usar disco de cuórum”
- Sección 2.10, “Adición de alta disponibilidad de Red Hat y SELinux”
- Sección 2.11, “Direcciones de multidifusión”
- Sección 2.12, “Tráfico unidifusión UDP”
- Sección 2.13, “Consideraciones para **`ricci`**”
- Sección 2.14, “Configuración de las máquinas virtuales en un entorno en clúster.”

2.1. Consideraciones generales de configuración

Puede configurar la adición de alta disponibilidad de Red Hat en una variedad de formas que se ajusten a sus necesidades. Tenga en cuenta las siguientes consideraciones generales cuando planee, configure e implemente su distribución.

Número de nodos de clúster soportados

El número máximo de nodos de clúster soportados por la adición de alta disponibilidad es 16.

Clústeres de un solo sitio

Únicamente los clústeres de un solo sitio son compatibles en este momento. Los clústeres esparcidos a través de varios lugares físicos no tienen soporte formal. Si desea obtener mayor información sobre clústeres multi-sitios, por favor contacte a su representante de soporte técnico de Red Hat.

GFS2

Aunque un sistema de archivos de GFS2 puede ser implementado en un sistema autónomo o como parte de una configuración de clúster, Red Hat no admite el uso de GFS2 como un sistema de archivos de nodo único. Red Hat es compatible con una serie de sistemas de archivos de nodo único de alto rendimiento que están optimizados para un solo nodo y por lo tanto, tienen generalmente menor sobrecarga que un sistema de archivos de clúster. Red Hat recomienda el uso de esos sistemas de archivos en lugar de GFS2 donde solo un nodo único se necesita montarse al sistema de archivos. Red Hat seguirá apoyando a los sistemas de archivos de GFS2 de nodo único para los clientes existentes.

Al configurar un sistema de archivos de GFS2 como un sistema de archivos de clúster, asegúrese de que todos los nodos del clúster tengan acceso al sistema de archivos compartidos. Las configuraciones de clúster asimétrico en las que algunos nodos tienen acceso al sistema de archivos y otros no, no tienen soporte. No se requiere en realidad que todos los nodos monten el sistema de archivos de GFS2.

Configuración de hardware de puntos únicos de falla

Los clústeres pueden incluir una matriz doble de controladores RAID, varios canales de red en condiciones de servidumbre, múltiples rutas entre los miembros del clúster y almacenaje y, sistemas de fuentes de alimentación ininterrumpibles y redundantes (UPS) para asegurarse de que no resulte ningún fallo en tiempo de inactividad de aplicaciones o pérdida de datos.

Como alternativa, se puede configurar un clúster de baja disponibilidad para proporcionar menos disponibilidad que la de un clúster de falla sin punto único. Por ejemplo, puede configurar un clúster con una matriz de discos RAID de controlador único y solamente un canal de Ethernet único.

Algunas alternativas de bajo costo, tales como controladores de RAID de host, RAID de software sin soporte de clúster y configuraciones SCSI paralelas de iniciador múltiple, no son compatibles o apropiadas para usar como almacenaje de clúster compartido.

Garantía de integridad de datos

Para garantizar la integridad de los datos, solo un nodo puede ejecutar un servicio de clúster y acceder a datos de servicio de clúster a la vez. El uso de interruptores en la configuración de hardware de clúster permite que un nodo alimente en ciclos a otro nodo antes de reiniciar los servicios de alta disponibilidad de ese nodo durante un proceso de conmutación. Esto impide que dos nodos accedan a los mismos datos de forma simultánea y los corrompan. Los *dispositivos de valla* (soluciones de hardware o software que encienden, apagan o reinician los nodos del clúster) se utilizan para garantizar la integridad de los datos en todas las condiciones de error.

Vinculación de canal Ethernet

El cuórum y la salud de nodo están determinados por la comunicación de mensajes entre nodos de clúster a través de Ethernet. Además, los nodos del clúster utilizan Ethernet para una variedad de funciones críticas del clúster (por ejemplo, cercado). Con el enlace de canal de Ethernet, múltiples interfaces Ethernet están configuradas para comportarse como una sola interfaz, lo cual reduce el riesgo de un único punto-de-falla en la conexión de Ethernet típica conectada entre nodos del clúster y otro hardware de clúster.

A partir de Red Hat Enterprise Linux 6.4, los modos de enlace 0, 1,y 2 tienen soporte.

IPv4 e IPv6

La adición de alta disponibilidad es compatible con protocolos IPv4 e IPv6 de Internet. El soporte de IPv6 en la adición de alta disponibilidad es nuevo para Red Hat Enterprise Linux 6.

2.2. Hardware compatible

Antes de configurar software de adición de alta disponibilidad de Red Hat, asegúrese de que su cluster use el hardware apropiado (por ejemplo, dispositivos de valla soportados, dispositivos de almacenaje e interruptores de canal de fibra). Consulte los lineamientos de configuración de hardware en http://www.redhat.com/cluster_suite/hardware/ para obtener la información más actualizada de compatibilidad de hardware.

2.3. Cómo habilitar puertos IP

Antes de implementar la adición de alta disponibilidad de Red Hat, debe habilitar ciertos puertos IP en los nodos de clúster y en computadores que ejecuten **luci** (el servidor de interfaz de usuario **Conga**). Las siguientes secciones identifican los puertos IP para ser habilitados:

- Sección 2.3.1, “Cómo habilitar puertos IP en nodos de clúster”
- Sección 2.3.2, “Activación del puerto IP para **luci**”

La siguiente sección proporciona las reglas `iptables` para habilitar los puertos que la adición de Alta disponibilidad de Red Hat necesita:

- Sección 2.3.3, “Cómo configurar el cortafuegos de iptables para permitir componentes de clúster”

2.3.1. Cómo habilitar puertos IP en nodos de clúster

Para que los nodos en un clúster puedan comunicarse entre sí, debe habilitar los puertos asignados a algunos componentes de adiciones de Alta disponibilidad de Red Hat. Tabla 2.1, “Puertos IP habilitados en nodos de adiciones de alta disponibilidad de Red Hat” lista los números de puertos IP, sus respectivos protocolos y los componentes a los cuales se asignan los números de puertos. En cada nodo de clúster, habilite los puertos IP según la Tabla 2.1, “Puertos IP habilitados en nodos de adiciones de alta disponibilidad de Red Hat”. Utilice `system-config-firewall` para activar los puertos IP.

Tabla 2.1. Puertos IP habilitados en nodos de adiciones de alta disponibilidad de Red Hat

Número de puerto IP	Protocolo	Componente
5404, 5405	UDP	`corosync/cman` (Gestor de clúster)
11111	TCP	`ricci` (propaga información de clúster actualizada)
21064	TCP	`dlm` (Gestor de bloqueo distribuido)
16851	TCP	`modclusterd`

2.3.2. Activación del puerto IP para luci

Para permitir que los computadores de cliente se comuniquen con un computador que ejecute **luci** (el servidor de interfaz de usuario **Conga**), debe habilitar el puerto IP asignado a **luci**. En cada equipo que ejecute **luci**, habilite el puerto IP según la Tabla 2.2, “Puertos IP habilitados en un computador que ejecuta luci”.

Nota

Si un nodo de clúster está ejecutando **luci**, el puerto 11111 debe haber sido ya habilitado.

Tabla 2.2. Puertos IP habilitados en un computador que ejecuta luci

Número de puerto IP	Protocolo	Componente
8084	TCP	**luci** (servidor de interfaz de usuario **Conga**)

A partir del lanzamiento de Red Hat Enterprise Linux 6.1, el cual activa la configuración mediante el archivo **/etc/sysconfig/luci**, puede especificamente configurar la dirección IP única en la que se sirve **luci**. Puede usar esta funcionalidad si su infraestructura incorpora más de una red y si desea acceder a **luci** desde la red interna únicamente. Para esto, descomente y modifique la línea en el archivo que especifica **host**. Por ejemplo, para cambiar la configuración de **host** en el archivo a 10.10.10.10, modifique la línea de **host** así:

```
host = 10.10.10.10
```

Para obtener mayor información sobre el archivo **/etc/sysconfig/luci**, consulte la Sección 2.4, "Configuración de **luci** con **/etc/sysconfig/luci**".

2.3.3. Cómo configurar el cortafuegos de iptables para permitir componentes de clúster

A continuación aparece un ejemplo de reglas IPtables para habilitar puertos IP que Red Hat Enterprise Linux 6 necesita (con la adición de Alta disponibilidad). Por favor observe que estos ejemplos usan 192.168.1.0/24 como subred, pero si usted utiliza estas reglas, deberá remplazar 192.168.1.0/24 por la subred apropiada.

Para **cman** (Gestor de clúster), use el siguiente filtraje.

```
$ iptables -I INPUT -m state --state NEW -m multiport -p udp -s 192.168.1.0/24
-d 192.168.1.0/24 --dports 5404,5405 -j ACCEPT
$ iptables -I INPUT -m addrtype --dst-type MULTICAST -m state --state NEW -m
multiport -p udp -s 192.168.1.0/24 --dports 5404,5405 -j ACCEPT
```

Para **dlm** (Gestor de bloqueo distribuido):

```
$ iptables -I INPUT -m state --state NEW -p tcp -s 192.168.1.0/24 -d
192.168.1.0/24 --dport 21064 -j ACCEPT
```

Para **ricci** (parte del agente remoto Conga):

```
$ iptables -I INPUT -m state --state NEW -p tcp -s 192.168.1.0/24 -d
192.168.1.0/24 --dport 11111 -j ACCEPT
```

Para **modclusterd** (parte del agente remoto de Conga):

```
$ iptables -I INPUT -m state --state NEW -p tcp -s 192.168.1.0/24 -d
192.168.1.0/24 --dport 16851 -j ACCEPT
```

Para **luci** (Servidor de interfaz de usuario de Conga):

```
$ iptables -I INPUT -m state --state NEW -p tcp -s 192.168.1.0/24 -d
192.168.1.0/24 --dport 16851 -j ACCEPT
```

Para **igmp** (Protocolo de administración de grupos en Internet):

```
$ iptables -I INPUT -p igmp -j ACCEPT
```

Después de ejecutar los comandos anteriores, guarde la configuración con el siguiente comando para que los cambios persistan después del rearranque:

```
$ service iptables save ; service iptables restart
```

2.4. Configuración de luci con /etc/sysconfig/luci

A partir del lanzamiento de Red Hat Enterprise Linux 6.1, puede configurar algunos aspectos de la conducta de **luci** mediante el archivo **/etc/sysconfig/luci**. Los parámetros que puede cambiar con este archivo incluyen los parámetros auxiliares del entorno en ejecución utilizados por el script init y la configuración de servidor. Además, puede modificar este archivo para ajustar algunos parámetros de configuración. Hay instrucciones dentro del archivo mismo que describen los parámetros de configuración que usted puede cambiar al modificar este archivo.

A fin de proteger el formato de destino, no cambie las líneas de no-configuración del archivo **/etc/sysconfig/luci**. Además, tenga cuidado al seguir la sintaxis requerida para este archivo, en particular para la sección **INITSCRIPT**, la cual no permite espacios en blanco alrededor del signo igual y requiere el uso de comillas para cerrar las cadenas que contienen espacios en blanco.

El ejemplo a continuación, muestra cómo cambiar el puerto que sirve a **luci** al modificar el archivo **/etc/sysconfig/luci**.

1. Descomente la siguiente línea en el archivo **/etc/cluster/cluster.conf**.

   ```
   #port = 4443
   ```

2. Remplace 4443 por el número del puerto deseado, el cual debe ser mayor que o igual a 1024 (no un puerto privilegiado). Por ejemplo, puede modificar esa línea del archivo como sigue para establecer el puerto a 8084 en el que se sirve **luci**.

   ```
   port = 8084
   ```

3. Reinicie el servicio de **luci** para que los cambios se efectúen.

Importante

Al modificar un parámetro de configuración en el archivo **/etc/sysconfig/luci** para redefinir un valor predeterminado, tenga cuidado al usar el nuevo valor en lugar del predeterminado descrito. Por ejemplo, si modifica el puerto que sirve a **luci**, asegúrese de haber especificado el valor que modificó al habilitar un puerto IP para **luci**, como se describe en la Sección 2.3.2, "Activación del puerto IP para **luci**".
El puerto modificado y los parámetros de host se reflejarán de forma automática en la URL que se despliega al iniciar el servicio de **luci**, como se describe en la Sección 3.2, "Inicio de **luci**". Debe utilizar esta URL para acceder a **luci**.

Para obtener una información más completa sobre los parámetros que puede configurar con el archivo **/etc/sysconfig/luci**, consulte la documentación dentro del propio archivo.

2.5. Cómo configurar ACPI para usar con dispositivos de valla integrados

Si su clúster usa dispositivos de valla integrados, debe configurar ACPI (Configuración avanzada e Interfaz de Energía) para asegurar cercado inmediato y completo.

Nota

Para obtener una información actual sobre dispositivos de vallas integrados soportado por la adición de alta disponibilidad de Red Hat, consulte http://www.redhat.com/cluster_suite/hardware/.

Si un nodo del clúster está configurado para ser cercado por un dispositivo integrado de valla, desactive ACPI soft-off para ese nodo. La desactivación de ACPI soft-off permite que un dispositivo de valla integrado desactive completamente un nodo de forma inmediata, en lugar de intentar un apagado limpio (por ejemplo, **shutdown -h now**). De otro modo, si ACPI soft-off, está habilitado, un dispositivo de valla integrado puede tardarse cuatro o más segundos para desactivar un nodo (por favor, consulte la siguiente nota). Además, si ACPI soft-off está activada y un nodo entra en pánico o se congela durante el cierre, el dispositivo de valla integrado no podrá desactivar el nodo. En esas circunstancias, el cercado se retarda o no se realiza. En consecuencia, cuando un nodo está cercado con un dispositivo de valla integrado y ACPI soft-off está activada, un clúster se recupera lentamente o requiere intervención administrativa para recuperarse.

Nota

La cantidad de tiempo necesario para cercar un nodo depende del dispositivo de valla integrado utilizado. Algunos dispositivos de valla integrada realizan el equivalente de presionar y sostener el botón de encendido; por lo tanto, el dispositivo de valla desactiva el nodo en cuatro o cinco segundos. Otros dispositivos de valla integrada realizan el equivalente de presionar el botón de encendido momentáneamente, confiando en que el sistema operativo desactive el nodo; por lo tanto, el dispositivo de valla desactiva el nodo en un lapso de tiempo de más de cuatro a cinco segundos.

Para desactivar ACPI Soft-Off, use la administración de **chkconfig** y verifique si el nodo se apaga inmediatamente después de que sea cercado. La forma preferida de desactivar ACPI Soft-Off es con administración **chkconfig**, sin embargo, si ese método no es satisfactorio para su clúster, puede desactivar ACPI Soft-Off con alguno de los métodos alternos dados a continuación:

- Cambiar la configuración de BIOS a "instant-off" o una configuración equivalente que apague el nodo sin demora

  

  Nota

  Desactivar ACPI Soft-Off con el BIOS no es posible en algunos computadores.

- Adición de **acpi=off** a la línea de comandos de arranque del kernel del archivo **/boot/grub/grub.conf**

  

  Importante

  Este método inhabilita completamente a ACPI; algunos computadores no arrancan correctamente si ACPI se inhabilita totalmente. Use este método *solamente* si otros métodos no son efectivos para su clúster.

Las siguientes secciones proporcionan procedimientos para el método preferido y métodos alternos de desactivación de ACPI Soft-Off:

- La Sección 2.5.1, “Desactivar ACPI Soft-Off con administración de **chkconfig** ” — Método preferido
- La Sección 2.5.2, “Desactivar ACPI Soft-Off con el BIOS” — Primer método alterno
- La Sección 2.5.3, “Desactivar completamente a ACPI en el archivo **grub.conf**” — Segundo método alterno

2.5.1. Desactivar ACPI Soft-Off con administración de chkconfig

Puede usar administración de **chkconfig** para desactivar ACPI Soft-Off ya sea quitando el demonio ACPI (**acpid**) de la administración de **chkconfig** o apagando **acpid**.

Nota

Este es el método preferido para desactivar ACPI Soft-Off.

Desactive ACPI Soft-Off con administración de **chkconfig** en cada nodo de clúster así:

1. Ejecute alguno de los comandos a continuación:
   - **chkconfig --del acpid** — Este comando remueve a **acpid** de la administración de **chkconfig**.

     — O —
   - **chkconfig --level 2345 acpid off** — Este comando apaga a **acpid**.
2. Reinicie el nodo.
3. Cuando el clúster esté configurado y ejecutándose, verifique si el nodo se apaga inmediatamente cuando está cercado.

   

   Nota

   Puede cercar al nodo con el comando **fence_node** o **Conga**.

2.5.2. Desactivar ACPI Soft-Off con el BIOS

Administración de **chkconfig** (Sección 2.5.1, "Desactivar ACPI Soft-Off con administración de **chkconfig** "), es el método preferido de desactivación de ACPI Soft-Off. Sin embargo, si el método preferido no es efectivo para su clúster, siga el procedimiento en esta sección.

Nota

Desactivar ACPI Soft-Off con el BIOS no es posible en algunos computadores.

Puede desactivar ACPI Soft-Off al configurar el BIOS de cada nodo de clúster así:

1. Reinicie el nodo e inicie el programa **BIOS CMOS Setup Utility**.
2. Navegue al menú de **Energía** (o el equivalente al menú de administración de energía).
3. En el menú de **Energía**, configure la función (o equivalente) **Soft-Off by PWR-BTTN** a **Apagado instantáneo** (o configuración equivalente que apague el nodo con el botón de energía sin demora). El Ejemplo 2.1, "**BIOS CMOS Setup Utility**: Soft-Off by PWR-BTTN se establece a Apagado instantáneo" muestra el menú **Energía** con la **Función ACPI** establecida a **Activada** y **Soft-Off by PWR-BTTN** establecida a **Apagado instantáneo**.

   

   Nota

   Los equivalentes a la **Función ACPI**, **Soft-Off by PWR-BTTN**,y **Apagado instantáneo** pueden variar entre computadores. Sin embargo, el objetivo de este procedimiento es el de configurar el BIOS para que el computador sea apagado a través del botón de energía sin demora.

4. Salga del programa **BIOS CMOS Setup Utility**, guardando la configuración de BIOS.
5. Cuando el clúster esté configurado y ejecutándose, verifique si el nodo se apaga inmediatamente cuando está cercado.

   

   Nota

   Puede cercar al nodo con el comando **fence_node** o **Conga**.

Ejemplo 2.1. BIOS CMOS Setup Utility: Soft-Off by PWR-BTTN se establece a Apagado instantáneo

```
+---------------------------------------------|-------------------+
|    ACPI Function             [Enabled]      |    Item Help      |
|    ACPI Suspend Type         [S1(POS)]      |-------------------|
|  x Run VGABIOS if S3 Resume   Auto          |   Menu Level   *  |
|    Suspend Mode              [Disabled]     |                   |
|    HDD Power Down            [Disabled]     |                   |
|    Soft-Off by PWR-BTTN      [Instant-Off   |                   |
|    CPU THRM-Throttling       [50.0%]        |                   |
|    Wake-Up by PCI card       [Enabled]      |                   |
|    Power On by Ring          [Enabled]      |                   |
|    Wake Up On LAN            [Enabled]      |                   |
|  x USB KB Wake-Up From S3     Disabled      |                   |
|    Resume by Alarm           [Disabled]     |                   |
|  x  Date(of Month) Alarm       0            |                   |
|  x  Time(hh:mm:ss) Alarm       0 :  0 :     |                   |
|    POWER ON Function         [BUTTON ONLY   |                   |
|  x KB Power ON Password       Enter         |                   |
|  x Hot Key Power ON           Ctrl-F1       |                   |
|                                             |                   |
|                                             |                   |
+---------------------------------------------|-------------------+
```

Este ejemplo muestra la **Función ACPI Activada**, y **Soft-Off by PWR-BTTN** en **Apagado instantáneo**.

2.5.3. Desactivar completamente a ACPI en el archivo `grub.conf`

La administración de **chkconfig** (Sección 2.5.1, "Desactivar ACPI Soft-Off con administración de **chkconfig** "), es el método preferido para desactivar ACPI Soft-Off. Si el método preferido no es efectivo para su clúster, puede desactivar ACPI Soft-Off con la administración de energía BIOS (Sección 2.5.2, "Desactivar ACPI Soft-Off con el BIOS"). Si ninguno de los dos métodos es efectivo para su clúster, puede desactivar ACPI completamente al añadir **acpi=off** a la línea de comandos de arranque de kernel en el archivo **grub.conf**.

Importante

Este método inhabilita completamente a ACPI; algunos computadores no arrancan correctamente si ACPI se inhabilita totalmente. Use este método *solamente* si otros métodos no son efectivos para su clúster.

Puede desactivar completamente a ACPI al editar el archivo **grub.conf** de cada nodo de clúster así:

1. Abra **/boot/grub/grub.conf** con el editor de textos.
2. Añada **acpi=off** a la línea de comandos de inicio del kernel en **/boot/grub/grub.conf** (consulte el Ejemplo 2.2, "Línea de comandos de arranque de Kernel con **acpi=off** añadida").
3. Reinicie el nodo.
4. Cuando el clúster esté configurado y ejecutándose, verifique si el nodo se apaga inmediatamente cuando está cercado.

Nota

Puede cercar al nodo con el comando **fence_node** o **Conga**.

Ejemplo 2.2. Línea de comandos de arranque de Kernel con acpi=off añadida

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/vg_doc01-lv_root
#          initrd /initrd-[generic-]version.img
#boot=/dev/hda
default=0
timeout=5
serial --unit=0 --speed=115200
terminal --timeout=5 serial console
title Red Hat Enterprise Linux Server (2.6.32-193.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-193.el6.x86_64 ro root=/dev/mapper/vg_doc01-
lv_root console=ttyS0,115200n8 acpi=off
        initrd /initramrs-2.6.32-131.0.15.el6.x86_64.img
```

En este ejemplo, **acpi=off** ha sido añadido a la línea de comandos de arranque del kernel — la línea que comienza por "kernel /vmlinuz-2.6.32-193.el6.x86_64.img".

2.6. Consideraciones para configurar servicios de alta disponibilidad

Puede crear un clúster para satisfacer sus necesidades de alta disponibilidad mediante la configuración de servicios de alta disponibilidad. El componente clave para la gestión de servicio de alta disponibilidad en la adición de alta disponibilidad de Red Hat, **rgmanager**, implementa conmutación en frío para aplicaciones fuera de la plataforma. En la adición de alta disponibilidad de Red Hat, se configura una aplicación con otros recursos de clúster para formar un servicio de alta disponibilidad que puede conmutar de un nodo del clúster a otro sin interrupción aparente a los clientes de clúster. Puede presentarse conmutación de Servicio de alta disponibilidad, si se presenta error en un nodo de clúster o si el administrador de sistema de clúster traslada el servicio de un nodo del clúster a otro (por ejemplo, para un corte de energía planeado de un nodo del clúster).

Para crear un servicio de alta disponibilidad, debe configurarlo en el archivo de configuración de cluster. Un servicio de alta disponibilidad comprende *recursos* de clúster. Los recursos de cluster construyen bloques que usted crea y maneja en el archivo de configuración de clúster — por ejemplo, una dirección IP, un script de inicialización de una aplicación o una partición compartida de GFS2 de Red Hat.

Un servicio de alta disponibilidad (HA) puede ejecutar solo en un nodo del clúster a la vez para mantener la integridad de los datos. Puede especificar la prioridad de conmutación en un dominio de conmutación, lo cual consiste en asignar un nivel de prioridad a cada nodo de un dominio de conmutación. El nivel de prioridad determina el orden de conmutación — al determinar qué nodo debe conmutar un servicio de alta disponibilidad. Si la prioridad de conmutación no se especifica, el servicio HA puede conmutar cualquier nodo en su dominio de conmutación. Además, puede especificar si el servicio solo se limita a ejecutar en los nodos de su dominio de conmutación asociado. (Cuando esté asociado a un dominio de conmutación sin restricciones, un servicio HA puede iniciar en cualquier nodo de clúster si ningún miembro de conmutación está disponible).

La Figura 2.1, “Ejemplo de servicio de clúster de servidor de red” muestra un ejemplo de un servicio de alta disponibilidad (HA), el cual es un servidor de red llamado "servidor de red de contenido". Se ejecuta en el nodo de clúster B y está en el dominio de conmutación que consta de nodos A, B y D. Además, el dominio de conmutación se configura con una prioridad de conmutar al nodo D antes del nodo A y, para restringir la conmutación para nodos solamente en ese dominio de conmutación. El servicio HA consta de estos recursos de clúster:

- Recurso de dirección IP — Dirección IP 10.10.10.201.
- Un recurso de aplicación llamado "httpd-content" — una aplicación de servidor de red init script **`/etc/init.d/httpd`** (especificando **`httpd`**).
- Un recurso de sistema de archivos — Red Hat GFS2 llamado "gfs2-content-webserver".

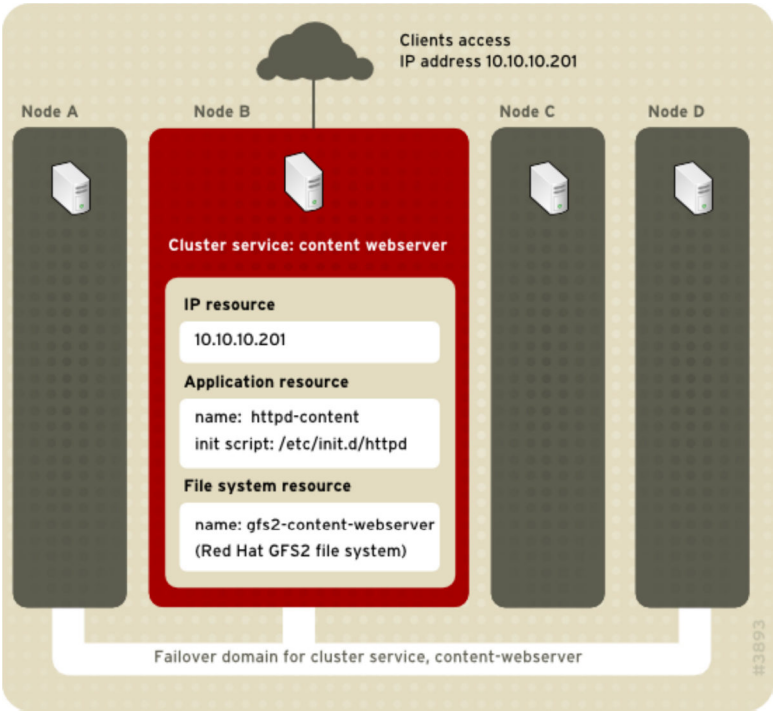

Figura 2.1. Ejemplo de servicio de clúster de servidor de red

Los clientes acceden al servicio de alta disponibilidad (HA) mediante la dirección IP 10.10.10.201, que habilita la interacción con la aplicación de servidor de red del contenido de httpd. La aplicación del contenido de httpd utiliza el sistema de archivos del servicio de red gfs2. Si el nodo B llegara a fallar, el servicio HA del servidor de red de contenido fallaría en el nodo D. Si el nodo D no estuviera disponible o también fallara, el servicio fallaría en el nodo A. La conmutación ocurriría con una interrupción de servicio mínima para los clientes de clúster. Por ejemplo, en un servicio HTTP, un cierto estado de información puede perderse (como datos de sesión). El servicio HA podría accederse desde otro nodo de clúster mediante la dirección IP que había antes de la conmutación.

Nota

Para obtener mayor información sobre servicios de alta disponibilidad y dominios de conmutación, consulte *Visión general de adición de alta disponibilidad*. Para obtener información sobre configuración de dominios de conmutación, consulte el Capítulo 3, *Configuración de adición de alta disponibilidad de Red Hat con **Conga*** (mediante **Conga**) o el Capítulo 7, *Configuración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos* (mediante herramientas de línea de comandos).

Un servicio de alta disponibilidad es un grupo de recursos de clúster configurado dentro de una entidad coherente que proporciona servicios especializados a clientes. Un servicio de alta disponibilidad se representa como un árbol de recursos en el archivo de configuración de clúster, **/etc/cluster/cluster.conf** (en cada nodo de cluster). En el archivo de configuración de clúster, cada árbol de recursos es una representación XML que especifica cada recurso, sus atributos y su relación con otros recursos en el árbol de recursos (relación de padre, hijos y hermanos).

Nota

Puesto que un servicio de alta disponibilidad consiste en recursos organizados dentro de un árbol jerárquico, el servicio se conoce algunas veces como *árbol de recursos* o *grupo de recursos*. Ambos nombres son sinónimos de *servicio de alta disponibilidad (HA)*.

En la raíz de cada árbol está un tipo de recurso — un *recurso de servicio*. Otros tipos de recursos comprenden el resto del servicio que determinan sus características. La configuración de un servicio de alta disponibilidad consiste en la creación de un recurso de servicio, la creación de recursos de clúster subordinados y la organización de ellos dentro de una entidad conforme a las restricciones jerárquicas del servicio.

Hay dos consideraciones importantes para tener en cuenta en la configuración de un servicio de alta disponibilidad:

- Los tipos de recursos necesarios para crear un servicio
- Relaciones padre, hijo y hermanos entre recursos

Los tipos de recursos y la jerarquía de recursos dependen del tipo de servicio que usted está configurando.

Los tipos de recursos de clúster están listados en el Apéndice B, *Parámetros de recursos de alta disponibilidad*. Información acerca de relaciones de padre, hijo y hermanos entre recursos aparece en el Apéndice C, *Comportamiento de recursos de alta disponibilidad*.

2.7. Validación de configuración

La configuración de clúster se valida automáticamente según el esquema del clúster en **/usr/share/cluster/cluster.rng** durante el tiempo de inicio y al recargar la configuración. También, puede validar una configuración de clúster en cualquier momento con el comando **ccs_config_validate**. Para obtener mayor información sobre validación de configuración al usar el comando **ccs**, consulte la Sección 5.1.6, “Validación de configuración”.

Un esquema anotado está disponible a la vista en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (por ejemplo **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Validación de configuración chequea los siguientes errores básicos:

- Validez XML — Verifica si archivo de configuración es un archivo XML válido.
- Opciones de configuración — Verifica si las opciones (elementos XML y atributos) son válidas.
- Valores de opción — Verifica si las opciones contienen datos válidos (limitados).

Los siguientes ejemplos muestran una configuración válida y configuraciones inválidas que ilustran los chequeos de validación:

- Configuración válida — Ejemplo 2.3, “Configuración de muestra **cluster.conf**: Archivo válido”
- XML inválido — Ejemplo 2.4, “Configuración de muestra **cluster.conf**: XML inválido”

- Opción inválida — Ejemplo 2.5, “Configuración de muestra **cluster.conf**: Opción inválida”
- Valor de opción inválido — Ejemplo 2.6, “**cluster.conf** Configuración de muestra: valor de opción inválido ”

Ejemplo 2.3. Configuración de muestra cluster.conf: Archivo válido

```
<cluster name="mycluster" config_version="1">
  <logging debug="off"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Ejemplo 2.4. Configuración de muestra cluster.conf: XML inválido

```
<cluster name="mycluster" config_version="1">
  <logging debug="off"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
<cluster>         <----------------INVALID
```

En este ejemplo, a la última línea de la configuración (anotada como "INVALID" aquí) le falta una barra oblicua — aparece **<cluster>** en lugar de **</cluster>**.

Ejemplo 2.5. Configuración de muestra `cluster.conf`: Opción inválida

```
<cluster name="mycluster" config_version="1">
  <loging debug="off"/>         <----------------INVALID
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
<cluster>
```

En este ejemplo, la segunda línea de configuración (anotada como "INVALID" aquí) contiene un elemento XML inválido — aparece como **`loging`** en lugar de **`logging`**.

Ejemplo 2.6. `cluster.conf` Configuración de muestra: valor de opción inválido

```
<cluster name="mycluster" config_version="1">
  <loging debug="off"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="-1">  <--------INVALID
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
<cluster>
```

En este ejemplo, la cuarta línea de configuración (anotada como "INVALID" aquí) contiene un valor inválido para el atributo XML, **`nodeid`** en la línea **`clusternode`** para **`node-01.example.com`**. El valor es un valor negativo ("-1") en lugar de un valor positivo ("1"). Para el atributo **`nodeid`**, el valor debe ser un valor positivo.

2.8. Consideraciones para NetworkManager

El uso de **NetworkManager** no está soportado en nodos de clúster. Si ha instalado **NetworkManager** en sus nodos de clúster, debe removerlo o desactivarlo.

Nota

El servicio **cman** no iniciará si **NetworkManager** está ejecutándose o ha sido configurado para ser ejecutado con el comando **chkconfig**.

2.9. Consideraciones para usar disco de cuórum

Disco de cuórum es un demonio de cuórum de disco, **qdiskd**, proporciona heurística adicional para determinar el estado de nodo. Con heurística puede determinar los factores que son importantes para la operación del nodo en el caso de una partición de red. Por ejemplo, en un clúster de cuatro nodos con una división de 3: 1, normalmente, los tres nodos "ganan" por mayoría de tres a uno. Bajo esas circunstancias, el nodo es cercado. No obstante, con **qdiskd**, puede configurar heurística que permita al nodo ganar en función de acceso a un recurso crítico (por ejemplo, una ruta de red crítica). Si el clúster requiere métodos adicionales para determinar la salud de nodo, debe configurar **qdiskd** para satisfacer esas necesidades.

Nota

La configuración de **qdiskd** no se requiere a menos que tenga los requerimientos especiales para salud de nodo. Un ejemplo de un requerimiento especial es una configuración "todo-menos-uno". En una configuración todo menos uno, **qdiskd** está configurado para proporcionar votos de cuórum suficientes para mantener cuórum a pesar de que solamente un nodo está funcionando.

Importante

En general, la heurística y otros parámetros **qdiskd** para su implementación dependen del entorno de sitio y requisitos especiales. Para entender el uso de la heurística y otros parámetros **qdiskd**, consulte la página de manual qdisk(5). Si necesita ayuda para entender y usar **qdiskd** para su sitio, contacte a un representante de soporte técnico autorizado de Red Hat.

Si necesita usar **qdiskd**, debe tener en cuenta lo siguiente:

Votos de nodo de clúster

Cuando utilice Quorum Disk, cada nodo de clúster debe tener un voto.

Valor de tiempo de espera de membresía de CMAN

El valor de tiempo de espera de membresía de CMAN (el tiempo que un nodo requiere para no responder antes de que CMAN lo considere muerto y no miembro) debe ser al menos el doble del valor de tiempo de espera de membresía de **qdiskd**. Esto se debe a que el demonio de cuórum debe detectar nodos fallidos por cuenta propia y puede tomar mucho más tiempo en hacerlo que CMAN. El valor predeterminado de tiempo de espera de membresía de CMAN es de 10 segundos. Otras condiciones específicas del sitio pueden afectar la relación entre los valores de tiempo de espera de CMAN y **qdiskd**. Para obtener ayuda sobre cómo ajustar el valor de tiempo de espera de membresía de CMAN, contacte a un representante de soporte técnico autorizado de Red Hat.

Valla

Para garantizar un cercado confiable al usar **qdiskd**, use valla de poder. Aunque otros tipos de vallas pueden ser fiables para cluster no configurados con **qdiskd**, no lo son para un cluster configurado con **qdiskd**.

Nodos máximos

Un clúster configurado con **qdiskd** soporta un máximo de 16 nodos. La razón de este límite es la escalabilidad; al aumentar el número de nodos, aumenta la cantidad de contención de E/S sincrónica en un dispositivo de disco de cuórum compartido.

Dispositivo de cuórum compartido

Un dispositivo de disco de cuórum debe ser un dispositivo de bloque compartido con acceso de lectura y escritura simultáneos por todos los nodos en un clúster. El tamaño mínimo del dispositivo de bloque es de 10 MB. Ejemplos de dispositivos de bloque compartido que pueden ser usados por **qdiskd** son matriz RAID SCSI multipuertos, un SAN de RAID de canal de fibra o un destino iSCSI de RAID configurado. Puede crear un dispositivo de disco de cuórum con **mkqdisk**, la herramienta de disco de cuórum de clúster. Para obtener información acerca de cómo usar la herramienta, consulte la página de manual (8) mkqdisk.

Nota

No se recomienda el uso de JBOD como un disco de cuórum. Un JBOD no puede proporcionar un rendimiento fiable y por lo tanto, no puede permitir que un nodo escriba en él con la suficiente rapidez. Si un nodo no puede escribir en un dispositivo de disco de cuórum con la suficiente rapidez, el nodo erróneamente es expulsado de un clúster.

2.10. Adición de alta disponibilidad de Red Hat y SELinux

La adición de alta disponibilidad para Red Hat Enterprise Linux 6 admite SELinux en el estado **impositivo** con el tipo de política de SELinux establecido a **targeted**.

Para obtener mayor información sobre SELinux, consulte la *Guía de implementación* de Red Hat Enterprise Linux 6.

2.11. Direcciones de multidifusión

Los nodos en un clúster se comunican entre sí mediante direcciones multidifusión. Por lo tanto, cada interruptor de red y equipo asociado en la adición de Alta disponibilidad de Red Hat debe configurarse para aceptar direcciones multidifusión y Protocolo de administración de grupos en Internet, IGMP. Verifique si cada interruptor de red y equipo de red asociados en la adición de Alta disponibilidad de Red Hat están habilitados. Sin mutlitidifusión ni IGMP, no todos los nodos, podrán participar en un clúster, lo que hará que el clúster falle; use unidifusión UDP en estos entornos, como se describe en la Sección 2.12, “Tráfico unidifusión UDP”.

Nota

Los procedimientos para configurar interruptores de red y equipo de red asociados varían según el producto. Consulte la documentación del proveedor correspondiente u otra información acerca de cómo configurar interruptores de red y el equipo de red asociado para habilitar direcciones de multidifusión e IGMP.

2.12. Tráfico unidifusión UDP

A partir del lanzamiento de Red Hat Enterprise Linux 6.2, los nodos en un clúster pueden comunicarse entre sí mediante el mecanismo de transporte de unidifusión UDP. Se recomienda, sin embargo, el uso de multidifusión IP para red de clúster. La unidifusión UDP es una alternativa que puede servir cuando multidifusión IP no está disponible.

Puede configurar la adición de alta disponibilidad de Red Hat para usar unidifusión UDP si configura el parámetro **cman transport="udpu"** en el archivo de configuración **cluster.conf**. También puede especificar unidifusión desde la página de **Configuración de red** de la interfaz de usuario **Conga** como se describe en la Sección 3.5.3, “Configuración de red”.

2.13. Consideraciones para `ricci`

Para Red Hat Enterprise Linux 6, **ricci**, remplaza a **ccsd**. Por lo tanto, es necesario que **ricci** esté ejecutándose en cada nodo de clúster para poder propagar información actualizada de configuración de clúster, ya sea a través del comando **cman_tool version -r**, el comando **ccs**, o el servidor de interfaz de usuario **luci**. Puede iniciar **ricci** mediante **service ricci start** o habilitándolo para que inicie en tiempo de arranque vía **chkconfig**. Para obtener información sobre cómo habilitar puertos IP para **ricci**, consulte la Sección 2.3.1, “Cómo habilitar puertos IP en nodos de clúster”.

Para el lanzamiento de Red Hat Enterprise Linux 6.1 y posteriores, el uso de **ricci** requiere una contraseña la primera vez que usted propaga configuración de clúster actualizada desde cualquier nodo. Configure su contraseña de **ricci** como root después de instalar **ricci** en su sistema con el comando **passwd ricci**, para usuario **ricci**.

2.14. Configuración de las máquinas virtuales en un entorno en clúster.

Al configurar su clúster con recursos de una máquina virtual, deberá usar las herramientas de **rgmanager** para iniciar y detener las máquinas virtuales. Si usa **virsh** para iniciar la máquina puede que la máquina virtual resulte en más de un sitio, lo cual puede causar daño de los datos en una máquina virtual.

Para reducir las posibilidades de que los administradores accidentalmente "inicien doble" las máquinas virtuales mediante las herramientas de clúster y no-clúster en un entorno agrupado, configure su sistema al almacenar los archivos de configuración de máquina virtual en alguna parte que no sea el sitio predeterminado. Al almacenar los archivos de configuración de máquina virtual en alguna parte diferente a la determinada, hará más difícil que por accidente inicie una máquina virtual con **virsh**, ya que el archivo de configuración será desconocido para **virsh** fuera de la caja.

El sitio no predeterminado para archivos de configuración de máquina virtual puede ser cualquiera. La ventaja de usar un recurso compartido de NFS o un sistema de archivos GFS2 compartido es que el administrador no necesita mantener los archivos de configuración en sincronización a través de los miembros del clúster. No obstante, se permite usar un directorio local siempre y cuando el administrador mantenga el contenido sincronizado de alguna manera en todo el clúster.

En la configuración de clúster, las máquinas virtuales pueden hacer referencia a este sitio no predeterminado mediante el atributo **path** de un recurso de máquina virtual. Observe que el atributo **path** es un directorio o set de directorios separados por el caracter de dos puntos ':' no una ruta a un archivo.

Aviso

El servicio **libvirt-guests** debe estar desactivado en todos los nodos que están ejecutando **rgmanager**. Si se autoinicia o reanuda una máquina virtual, puede que la máquina virtual resulte en más de un sitio, el cual puede hacer que los datos se dañen en la máquina virtual.

Para obtener mayor información sobre los atributos de recursos de una máquina virtual, consulte la Tabla B.24, “Máquina virtual”.

Capítulo 3. Configuración de adición de alta disponibilidad de Red Hat con Conga

3.1. Tareas de configuración

3.2. Inicio de luci

3.3. Cómo controlar el acceso a luci

3.4. Cómo crear un clúster

3.5. Propiedades globales de clúster
- 3.5.1. Propiedades generales de configuración
- 3.5.2. Configuración de propiedades de demonio de valla
- 3.5.3. Configuración de red
- 3.5.4. Cómo configura el protocolo de anillos redundantes
- 3.5.5. Configuración de disco de cuórum
- 3.5.6. Configuración de registro

3.6. Configuración de dispositivos de valla
- 3.6.1. Cómo crear un dispositivo de valla
- 3.6.2. Modificación de un dispositivo de valla
- 3.6.3. Borrado de un dispositivo de valla

3.7. Configuración de cercado para miembros de clúster
- 3.7.1. Configuración de un dispositivo de vallas único para un nodo
- 3.7.2. Configuración de un dispositivo de vallas de respaldo
- 3.7.3. Configuración de un nodo con energía redundante

3.8. Configuración de dominio de conmutación
- 3.8.1. Adición de un dominio de conmutación
- 3.8.2. Modificación de un dominio de conmutación
- 3.8.3. Borrado de un dominio de conmutación

3.9. Configuración de recursos de clúster globales

3.10. Adición de un servicio de clúster al clúster

Este capítulo describe cómo configurar software de adición de alta disponibilidad de Red Hat con **Conga**. Para obtener información sobre el uso de **Conga** para administrar un clúster en ejecución, consulte el Capítulo 4, *Administración de adición de alta disponibilidad de Red Hat con **Conga***.

Nota

Conga es una interfaz gráfica de usuario que sirve para administrar la adición de alta disponibilidad de Red Hat. Observe, no obstante, que para usar efectivamente la interfaz usted necesita tener un buen conocimiento de los conceptos subyacentes. No se recomienda aprender a configurar mediante la exploración de funcionalidades disponibles en la interfaz, ya que puede que el sistema no sea lo suficientemente sólido para mantener todos los servicios en ejecución cuando los componentes fallan.

Este capítulo consta de las siguientes secciones:

- Sección 3.1, “Tareas de configuración”
- Sección 3.2, “Inicio de **luci**”
- Sección 3.3, “Cómo controlar el acceso a luci”
- Sección 3.4, “Cómo crear un clúster”
- Sección 3.5, “Propiedades globales de clúster”
- Sección 3.6, “Configuración de dispositivos de valla”
- Sección 3.7, “Configuración de cercado para miembros de clúster”
- Sección 3.8, “Configuración de dominio de conmutación”
- Sección 3.9, “Configuración de recursos de clúster globales”
- Sección 3.10, “Adición de un servicio de clúster al clúster”

3.1. Tareas de configuración

La configuración de software de adición de alta disponibilidad de Red Hat mediante **Conga** consta de los siguientes pasos:

1. Configuración y ejecución de la interfaz de usuario de configuración de **Conga** — el servidor

luci. Consulte la Sección 3.2, “Inicio de **luci**”.

2. Creación de un clúster. Consulte la Sección 3.4, “Cómo crear un clúster”.
3. Configuración de propiedades de clúster globales. Consulte la Sección 3.5, “Propiedades globales de clúster”.
4. Configuración de dispositivos de valla. Consulte la Sección 3.6, “Configuración de dispositivos de valla”.
5. Configuración de cercado para miembros de clúster. Consulte la Sección 3.7, “Configuración de cercado para miembros de clúster”.
6. Creación de dominios de conmutación. Consulte la Sección 3.8, “Configuración de dominio de conmutación”.
7. Creación de recursos. Consulte la Sección 3.9, “Configuración de recursos de clúster globales”.
8. Creación de servicios de clúster. Consulte la Sección 3.10, “Adición de un servicio de clúster al clúster”.

3.2. Inicio de luci

Instalación de ricci

El uso de **luci** para configurar un clúster requiere que **ricci** esté instalado y en ejecución en los nodos de clúster como se describe en la Sección 2.13, “Consideraciones para **ricci**”. Como se anota en esa sección, al usar **ricci** requerirá la contraseña que **luci** le pide que ingrese para cada nodo cuando usted crea un clúster, descrito en la Sección 3.4, “Cómo crear un clúster”.
Antes de iniciar a **luci**, verifique si los puertos IP en sus nodos de clúster permiten conexiones al puerto 11111 desde el servidor de **luci** en los nodos con que **luci** se esté comunicando. Para obtener mayor información sobre cómo habilitar puertos IP en nodos de clúster, consulte la Sección 2.3.1, “Cómo habilitar puertos IP en nodos de clúster”.

Para administrar la adición de alta disponibilidad de Red Hat con **Conga**, instale y ejecute **luci** así:

1. Seleccione un computador para albergar a **luci** e instale el software de **luci** es ese equipo. Por ejemplo:

```
# yum install luci
```

Nota

Por lo general, un computador en una jaula de servidor o un centro de datos alberga a **luci**; no obstante, un computador de clúster también puede albergar a **luci**.

2. Inicie a **luci** mediante **service luci start**. Por ejemplo:

```
# service luci start
Starting luci: generating https SSL certificates...  done
                                                           [  OK  ]

Please, point your web browser to https://nano-01:8084 to access luci
```

Nota

A partir del lanzamiento de Red Hat Enterprise Linux 6.1, usted puede configurar algunos aspectos de la conducta de **luci** mediante el archivo **/etc/sysconfig/luci**, que incluye los parámetros de puerto y host, así como se describe en la Sección 2.4, “Configuración de **luci** con **/etc/sysconfig/luci**”. Los parámetros de puerto y host modificados se reflejarán en la URL cuando inicie el servicio **luci**.

3. En un navegador, escriba la URL del servidor **luci** en la cajilla de dirección de URL y haga clic en **Ir** (o el equivalente). La sintaxis de URL para el servidor **luci** es **https://*luci_server_hostname*:*luci_server_port***. El valor predeterminado de ***luci_server_port*** es **8084**.

   La primera vez que usted acceda a **luci**, se desplegará un indicador específico de navegador de red sobre el Certificado SSL autofirmado (del servidor de **luci**). Tras reconocer el cuadro de diálogo o cuadros, su navegador desplegará la página de inicio de sesión de **luci**.

4. Aunque cualquier usuario capaz de autenticarse en el sistema que alberga **luci** puede ingresar a **luci**, a partir del lanzamiento de Red Hat Enterprise Linux 6.2 solo el usuario root en el sistema que esté ejecutando **luci** puede acceder a cualquiera de los componentes de **luci** hasta que un administrador (el usuario root u otro usuario con permisos de administrador) establezca los permisos para ese usuario. Para obtener información sobre cómo establecer permisos de **luci** para usuarios, consulte la Sección 3.3, "Cómo controlar el acceso a luci".

   Al ingresar a **luci** se despliega la página de **Base de origen** de **luci**, como se muestra en la Figura 3.1, "Página de base de origen de luci".

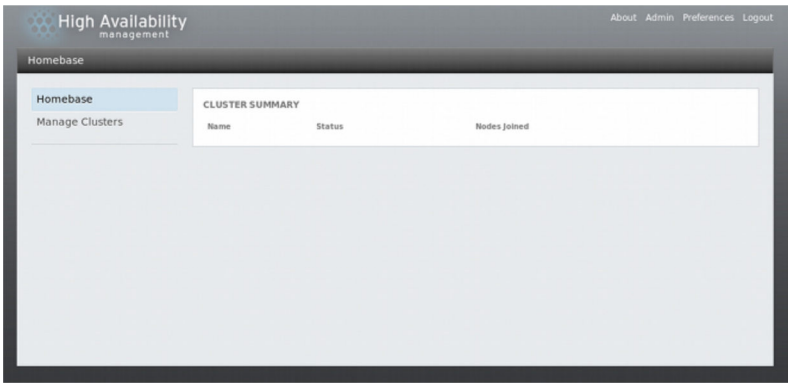

Figura 3.1. Página de base de origen de luci

Nota

Hay un tiempo de expiración para **luci** que saca al usuario después de 15 minutos de inactividad.

3.3. Cómo controlar el acceso a luci

Desde el lanzamiento de Red Hat Enterprise Linux 6, se han agregado las siguientes funcionalidades a la página de **Usuarios y permisos**.

- A partir de Red Hat Enterprise Linux 6.3, el usuario root o a quien se le hayan otorgado permisos administrativos de **luci** en un sistema que ejecute **luci** puede controlar el acceso a varios componentes de **luci** al establecer los permisos para usuarios individuales en un sistema.
- A partir de Red Hat Enterprise Linux 6.3, el usuario root o aquel a quien se le han otorgado permisos administrativos de **luci** también puede usar la interfaz de **luci** para añadir usuarios al sistema.
- A partir de Red Hat Enterprise Linux 6.4, el usuario root o aquel a quien se le hayan otorgado permisos administrativos de **luci** también puede usar la interfaz de **luci** para borrar usuarios del sistema.

Para agregar usuarios, borrar usuarios o establecer permisos de usuarios, ingrese a **luci** como `root` o como el usuario a quien se la hayan otorgado permisos administrativos y haga clic en **Admin** en la esquina superior derecha de la pantalla de **luci**. y así desplegará la página de **Usuarios y permisos**, la cual muestra los usuarios existentes.

Para borrar usuarios, seleccione el usuario o los usuarios y haga clic en `Borrar seleccionado`.

Para agregar un usuario, haga clic en `Añadir un usuario` e ingrese el nombre del usuario que desea agregar.

Para establecer o cambiar permisos para un usuario, seleccione el usuario desde el menú desplegable en **Permisos de usuario**. Esto le permitirá establecer los siguientes permisos:

`Luci Administrator`

Otorga al usuario los mismos permisos que tiene el usuario root, con todos los permisos en todos los clúster y la capacidad de dar o quitar permisos de los otros usuarios a excepción de root, cuyos permisos no se pueden limitar.

Puede crear clústeres

Permite al usuario crear nuevos clústeres, como se describe en la Sección 3.4, “Cómo crear un clúster”.

Puede importar clústeres existentes

Permite al usuario añadir un clúster existente a la interfaz de **luci** como se describe en la Sección 4.1, “Añadir un clúster existente a la interfaz luci”.

Para cada clúster que haya sido creado o importado a **luci**, puede establecer los siguientes permisos para el usuario indicado:

Puede ver este clúster

Permite al usuario ver el clúster especificado.

Puede cambiar la configuración de clúster

Permite al usuario modificar la configuración para el clúster especificado, a excepción de la adicionar o retirar nodos de clúster.

Puede activar, desactivar, reubicar y migrar grupos de servicios

Permite al usuario manejar servicios de alta disponibilidad, como se describe en la Sección 4.5, “Administrar servicios de alta disponibilidad”.

Puede detener, iniciar y reiniciar nodos de clúster

Permite al usuario administrar nodos individuales de un clúster, como se describe en la Sección 4.3, “Administrar nodos de clúster”.

Puede añadir y borrar nodos

Permite al usuario añadir o borrar nodos de un clúster, como se describe en la Sección 3.4, “Cómo crear un clúster”.

Puede retirar este clúster de luci

Permite al usuario quitar y borrar un clúster desde la interfaz **luci**, como se describe en la Sección 4.4, “Iniciar, parar, reiniciar, y borrar clústeres”.

Haga clic en **Enviar** para que los permisos se efectúen, o haga clic en **Restablecer** para volver a los valores iniciales.

3.4. Cómo crear un clúster

La creación de un clúster con **luci** consiste en nombrar un clúster, añadir nodos de clúster al clúster, ingresar sus contraseñas de **ricci** para cada nodo y enviar la solicitud para crear un clúster. Si la información de nodos y contraseñas están correctas, **Conga** instalará automáticamente software en los nodos de clúster (si los paquetes de software apropiados no están instalados correctamente) e iniciará el clúster. Cree un clúster así:

1. Haga clic en **Administrar clúster** del menú de **luci**, a la izquierda de la página de **Base de origen**. La pantalla de **Clústeres** aparecerá, como se muestra en la Figura 3.2, “Página de administración de clúster de luci”.

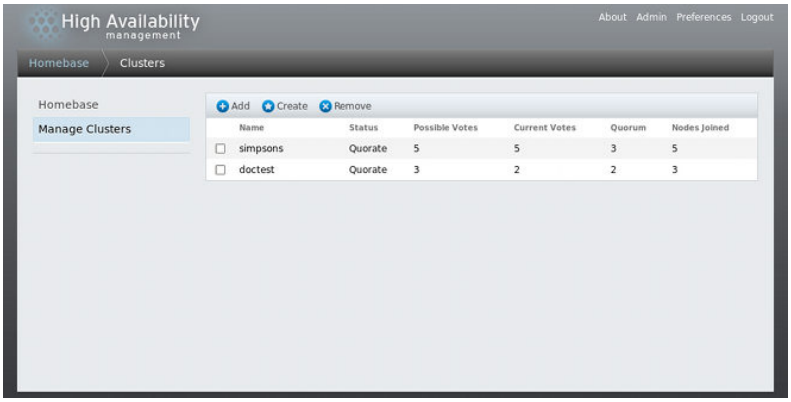

Figura 3.2. Página de administración de clúster de luci

2. Haga clic en **Crear**. La pantalla de **Crear un nuevo clúster** aparecerá, como se muestra en la Figura 3.3, "Cuadro de diálogo de creación de clúster luci".

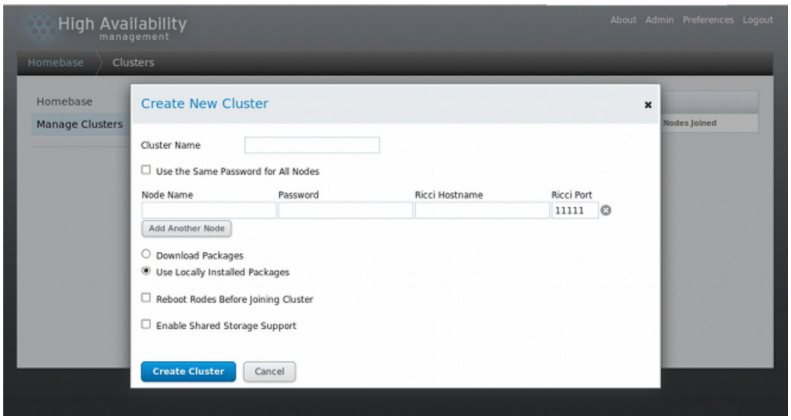

Figura 3.3. Cuadro de diálogo de creación de clúster luci

3. Ingrese los siguientes parámetros en el cuadro de diálogo **Crear un nuevo clúster**, si es necesario:
   - En la casilla de texto **Nombre de clúster**, ingrese un nombre de clúster. El nombre de clúster no puede exceder 15 caracteres.
   - Si cada nodo en el clúster tiene la misma contraseña de **ricci**, puede marcar **Usar la misma contraseña para todos los nodos** para autocompletar el campo de **contraseña** al añadir nodos.
   - Ingrese el nombre de nodo para un nodo en el clúster en la columna **Nombre de nodo** e ingrese la contraseña de **ricci** para el nodo en la columna de **Contraseña**.
   - Si su sistema está configurado con una red privada dedicada que es utilizada únicamente por el tráfico del clúster, puede configurar **luci** para que se comunique con **ricci** en una dirección diferente a la cual el nombre de nodo de clúster se resuelve. Puede hacerlo si ingresa la dirección como **Nombre de host de Ricci**.
   - Si está utilizando un puerto para el agente **ricci** diferente al predeterminado 11111, puede cambiar ese parámetro.
   - Haga clic en **Añadir otro nodo** e ingrese el nombre de nodo y la contraseña de **ricci** para cada nodo adicional en el clúster.
   - Si no desea actualizar los paquetes de software que ya están instalados en los nodos cuando crea el clúster, deje la opción **Usar paquetes instalados localmente** seleccionada. Si desea actualizar todos los paquetes de software de clúster, seleccione la opción **Descargar paquetes**.

Nota

Si al seleccionar la opción **Usar paquetes instalados localmente** o **Descargar paquetes**, alguno de los componentes de clúster básicos faltan (`cman`, `rgmanager`, `modcluster` y todas sus dependencias), serán instalados. Si no pueden ser instalados, la creación de nodo fallará.

- Seleccione **Nodos de reinicio antes de conectar el clúster** si se desea.
- Seleccione **Habilitar el soporte de almacenamiento compartido** si el almacenamiento en clúster se requiere. Así, descarga los paquetes para soporte de almacenamiento en clúster y activa LVM en clúster. Debe seleccionarlo solamente cuando tenga acceso a la adición de almacenamiento resistente o a la adición de sistema de archivos escalables.

4. Haga clic en `Crear clúster`. Al hacer clic en `Crear clúster` se producen las siguientes acciones:
   a. Si ha seleccionado **Descargar paquetes**, los paquetes de software de clúster se descargarán en los nodos.
   b. El software de clúster se instala en los nodos (o se verifica que los paquetes de software instalados sean apropiados).
   c. El archivo de configuración de clúster se actualiza y propaga para cada nodo en el clúster.
   d. Los nodos añadidos se conectan al clúster.

   Aparece un mensaje que dice que se está creando el clúster. Cuando el clúster está listo, la pantalla muestra el estatus del clúster recién creado, como se muestra en la Figura 3.4, "Pantalla de nodo de clúster". Observe que si **ricci** no se está ejecutando en ninguno de los nodos, la creación de clúster fallará.

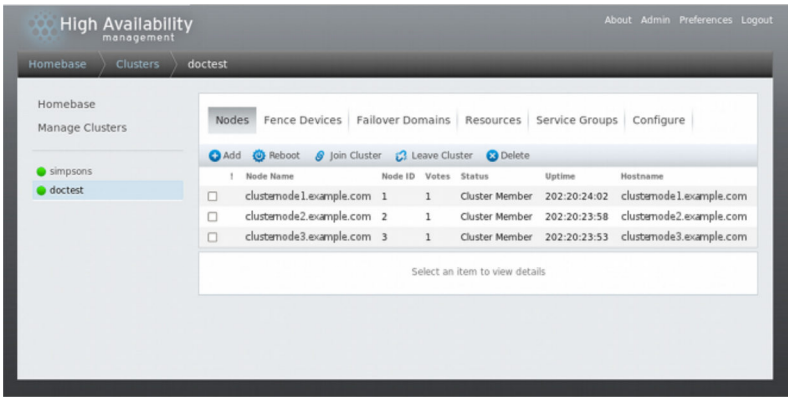

Figura 3.4. Pantalla de nodo de clúster

5. Después de hacer clic en `Crear clúster`, puede añadir o borrar nodos del clúster haciendo clic en la función **Añadir** o **Borrar** desde el menú en la parte superior de la página de pantalla de nodo de clúster. A menos que usted esté borrando un nodo completo, se deben detener los nodos antes de borrarlos. Para obtener mayor información sobre cómo borrar un nodo de un clúster existente que está en ejecución, consulte la Sección 4.3.4, "Borrado de un miembro de un clúster".

Nota

El retiro de un nodo de clúster del clúster es una operación destructiva que no puede deshacerse.

3.5. Propiedades globales de clúster

Cuando selecciona el clúster que va a configurar, se desplegará una página específica de clúster. La página proporciona una interfaz para configurar las propiedades de todo el clúster. Puede configurar las propiedades de todo el clúster al hacer clic en **Configurar** en la parte superior de la pantalla del clúster. Esto produce una interfaz etiquetada que proporciona las siguientes etiquetas: **General**, **Demonio de vallas**, **Red**, **Redundant Ring**, **QDisk** y **Ingreso**. Para configurar los parámetros en esas etiquetas, ignore la sección para esa pestaña.

3.5.1. Propiedades generales de configuración

Al hacer clic en la pestaña **General** aparecerá la página de **Propiedades generales**, la cual proporciona una interfaz para modificar la versión de configuración.

- La casilla de texto **Nombre de clúster** muestra el nombre de clúster; no acepta un cambio de nombre de clúster. La única forma de cambiar el nombre de un clúster es crear una nueva configuración de clúster con el nuevo nombre.
- El valor de **versión de configuración** se establece a `1` y aumenta automáticamente cada vez que usted modifica la configuración de clúster. Sin embargo, si necesita establecerlo a otro valor, puede especificarlo en la casilla de texto de **Versión de configuración**.

Si ha cambiado el valor de **Versión de configuración**, haga clic en **`Aplicar`** para que este cambio se efectúe.

3.5.2. Configuración de propiedades de demonio de valla

Al hacer clic en la pestaña **Demonio de valla** aparece la página **Propiedades de demonio de valla**, la cual proporciona una interfaz para configurar **Retraso de posfalla**y **Retraso de posconexión**. Los valores que usted configura para estos parámetros son propiedades generales de cercado para el clúster. Para configurar los dispositivos de valla específicos para los nodos del clúster, use el elemento del menú **Dispositivos de valla** de la pantalla de clúster, como se describe en la Sección 3.6, “Configuración de dispositivos de valla”.

- El parámetro de **Retraso de postfalla** es el número de segundos que un demonio de valla (**`fenced`**) espera antes de cercar un nodo (un miembro de dominio de valla) después de que el nodo ha fallado. El **Retraso de postfalla** es `0`. Su valor puede cambiarse para ajustarse al clúster y al rendimiento de red.
- El parámetro de **Retraso de posconexión** es el número de segundos que el demonio de valla (**`fenced`**) espera antes de cercar un nodo después de que el nodo se enlace al dominio. El valor predeterminado del **Retraso de posconexión** es `6`. Un parámetro típico para **Retraso posconexión** está entre 20 y 30 segundos, pero puede variar según el rendimiento del clúster y de la red.

Ingrese los valores requeridos y haga clic en **`Aplicar`** para que los cambios se efectúen.

Nota

Para obtener mayor información sobre el **Retraso de posconexión** y el **Retraso de posfalla**, consulte la página de manual fenced(8).

3.5.3. Configuración de red

La pestaña de **Red** muestra la página de **Configuración de red**, la cual proporciona una interfaz para configurar el tipo de transporte de red.

Puede utilizar esta pestaña para seleccionar una del siguientes opciones:

- **Multidifunda UDP y permita al clúster elegir la dirección de multidifusión**

  Esta es una configuración predeterminada. Con esta opción seleccionada, el software de adición de alta disponibilidad de Red Hat crea una dirección multidifusión basada en el identificador de clúster. Genera los 16 bits inferiores de la dirección y los agrega a la parte superior de la dirección dependiendo de si el protocolo IP es IPv4 o IPv6:
  - Para IPV4 — La dirección formada es 239.192. más los 16 bits inferiores generados por el software de adición de alta disponibilidad de Red Hat.
  - Para IPV6 — La dirección formada es FF15:: más los 16 bits inferiores generados por el software de adición de alta disponibilidad de Red Hat.

  

  Nota

  El identificador de clúster es un identificador único que **`cman`** genera para cada clúster. Para ver el ID de clúster, ejecute el comando **`cman_tool status`** en el nodo de clúster.

- **Multidifunda UDP y especifique manualmente la dirección de multidifusión**

  Si necesita usar la dirección específica de multidifusión, seleccione esta opción para ingresar a una dirección multidifusión en el cuadro de texto **Dirección de multidifusión**.

Si usted sí especifica una dirección de multidifusión, deberá usar las series 239.192.x.x (o FF15:: para IPv6) que emplea **cman**. De lo contrario, el uso de dirección de multidifusión fuera de este rango puede producir resultados impredecibles. Por ejemplo, con 224.0.0.x (el cual es "Todos los hosts en la red") no se pueden poner en la ruta de forma correcta o incluso,de ninguna forma por algún hardware.

Si especifica o modifica una dirección multidifusión, debe reiniciar el clúster para que el cambio se efectúe. Para obtener mayor información sobre cómo iniciar y detener un clúster con **Conga**, consulte la Sección 4.4, “Iniciar, parar, reiniciar, y borrar clústeres”.

Nota

Si especifica una dirección de multidifusión, asegúrese de comprobar la configuración de enrutadores que pasan los paquetes de clúster. Algunos enrutadores pueden tardar mucho tiempo en aprender direcciones, lo cual afecta seriamente el rendimiento del clúster.

- **UDP Unicast (UDPU)**

  A partir del lanzamiento de Red Hat Enterprise Linux 6.2, los nodos en un clúster pueden comunicarse entre sí mediante el mecanismo de transporte de unidifusión UDP. Se recomienda, sin embargo, el uso de multidifusión IP para red de clúster. Unidifusión UDP es una alternativa que puede servir cuando multidifusión IP no está disponible. No se recomienda para implementaciones de GFS2 mediante unidifusión UDP.

Haga clic en **Aplicar**. Cuando cambie el tipo de transporte, se necesita reiniciar un clúster para que los cambios se efectúen.

3.5.4. Cómo configura el protocolo de anillos redundantes

A partir de Red Hat Enterprise Linux 6.4, la adición de Alta disponibilidad de Red Hat soporta la configuración del protocolo de anillos redundantes. Cuando utilice el protocolo de anillos redundantes, se debe tener en cuenta un gran número de consideraciones como se describe en la Sección 7.6, “Cómo configura el protocolo de anillos redundantes”.

Al hacer clic en la pestaña **Anillo redundante** se despliega la página **Configuración de protocolo de anillo redundante**. Esta página muestra todos los nodos que están configurados actualmente para el clúster. Si va a configurar un sistema para que use el protocolo de anillo redundante, debe especificar el **Nombre alternativo** para cada nodo para el segundo anillo.

La página de **Configuración de protocolo de anillo redundante** permite también especificar la **Dirección multidifusión de anillo alterno**, el **Puerto CMAN de anillo alterno**, y el **TTL de Paquete multidifusión de anillo alterno** para el segundo anillo.

Si especifica una dirección multidifusión para el segundo anillo, la dirección multidifusión alterna o el puerto alterno debe ser diferente a la dirección multidifusión para el primer anillo. Si especifica un puerto alterno, los números de puerto del primer anillo y el segundo anillo deben diferir en al menos 2, puesto que el sistema mismo usa 'Port' y 'Port -1' para realizar operaciones. Si no desea especificar una dirección multidifusión, el sistema usará automáticamente la dirección multidifusión para el segundo anillo.

3.5.5. Configuración de disco de cuórum

Al hacer clic en la pestaña **QDisk** aparece la página de **Configuración de disco de cuórum**, la cual proporciona una interfaz para configurar parámetros de disco de cuórum en caso de que necesite usar un disco de cuórum.

Importante

Los parámetros de disco de cuórum y heurística dependen del entorno de sitio y de los requisitos especiales. Para entender el uso de parámetros de disco de cuórum y heurística, consulte la página de manual qdisk(5). Si requiere asistencia para entender y usar disco de cuórum, contacte al representante autorizado de Red Hat.

El parámetro **No utilizar disco de cuórum** está activado por defecto. Si necesita usar un disco de cuórum, haga clic en **Usar un disco de cuórum**, ingrese los parámetros de disco de cuórum, haga clic en **Aplicar**, y reinicie el clúster para que los cambios se efectúen.

Tabla 3.1, “Parámetros de disco de cuórum” describe los parámetros de disco de cuórum.

Tabla 3.1. Parámetros de disco de cuórum

Parámetro	Descripción
Especificar un dispositivo físico: Por etiqueta de dispositivo	Especifica la etiqueta de disco de cuórum por la herramienta `mkqdisk`. Si este campo se utiliza, el demonio de cuórum lee el archivo `/proc/partitions` y verifica las firmas de qdisk en cada bloque hallado con la etiqueta especificada. Esto es útil en configuraciones en las que el nombre de dispositivo de cuórum difiere entre nodos.
Heurística	**Ruta al programa** — El programa utilizado para determinar si esta heurística está disponible. Puede ser cualquiera que pueda ser ejecutada por `/bin/sh -c`. Un valor de retorno de 0 indica éxito; cualquier otro indica falla. Este campo es obligatorio. **Intervalo** — La frecuencia (en segundos) en la cual se consulta la heurística. El intervalo predeterminado para cada heurística es 2 segundos. **Puntaje** — El valor de la heurística. Tenga cuidado al determinar puntajes para heurística. El puntaje predeterminado para cada heurística es 1. **TKO** — El número de fallas consecutivas requeridas antes de que esta heurística se declare no disponible.
Puntaje total mínimo	El puntaje mínimo para que un nodo sea considerado "vivo". Si se omite o establece a 0, la función predeterminada, `floor((n+1)/2)`, se utiliza, donde *n* es la suma de puntajes de heurística. El valor de **Puntaje total mínimo** nunca debe exceder la suma de los puntajes de heurística; de lo contrario, el disco de cuórum no puede estar disponible.

Nota

Al hacer clic en **Aplicar** en la pestaña **Configuración de QDisk** se propagarán los cambios al archivo de configuración de cluster (`/etc/cluster/cluster.conf`) en cada nodo de clúster. Sin embargo, para que el disco de cuórum funcione o para hacer algunas modificaciones (consulte la Sección 4.4, “Iniciar, parar, reiniciar, y borrar clústeres”), asegurándose de haber reiniciado el demonio `qdiskd` en cada nodo.

3.5.6. Configuración de registro

Al hacer clic en la pestaña **Registro** aparece la página de **Configuración de registro**, la cual proporciona una interfaz para configurar parámetros de registro.

Puede configurar los siguientes parámetros para configuración de ingreso global:

- La revisión del **Registro de mensajes de depuración** habilita mensajes de depuración en el archivo de registro.
- La revisión de **Mensajes de registro a syslog** habilita los mensajes a `syslog`. Puede seleccionar **Herramienta de mensajes syslog** y **Prioridad de mensajes de syslog**. La configuración de **Prioridad de mensajes de syslog** indica que los mensajes en el nivel seleccionado y superior se envían a `syslog`.
- La revisión de **Mensajes de registro para archivo de registro** habilita los mensajes para el archivo de registro. Usted puede especificar el nombre de **Ruta de archivo de registro**. El parámetro **Prioridad de mensajes de logfile** indica que los mensajes en el nivel seleccionado y superior se guardan en el archivo de registro.

Puede sobrescribir los parámetros globales de ingreso para demonios específicos si selecciona uno de los demonios en la parte inferior de la página **Sobrescribir registro de demonio específico** en debajo de la página de **Configuración de registro**. Después de seleccionar el demonio, puede verificar también si registra o no los mensajes de depuración para ese demonio específico. También puede especificar el `syslog` y los parámetros de archivo de registro para ese demonio.

Haga clic en `Aplicar` para que los cambios de configuración de ingreso especificados se efectúen.

3.6. Configuración de dispositivos de valla

La configuración de dispositivos de vallas consiste en crear, actualizar y borrar dispositivos de vallas para el clúster. Debe configurar los dispositivos de vallas en un clúster antes de configurar el cercado para los nodos en el clúster.

La creación de un dispositivo de valla consiste en seleccionar un tipo de dispositivo de valla e ingresar parámetros para ese dispositivo de valla (por ejemplo, nombre, dirección IP, inicio de sesión y contraseña). La actualización de un dispositivo de valla consiste en seleccionar un dispositivo de valla existente y cambiar los parámetros para ese dispositivo de valla. La eliminación de un dispositivo de valla consiste en seleccionar un dispositivo existente de la valla y la eliminación.

Esta sección provee procedimientos para las siguientes tareas:

- La creación de dispositivos de valla — Consulte la Sección 3.6.1, “Cómo crear un dispositivo de valla”. Cuando haya creado y nombrado un dispositivo de valla, puede configurar los dispositivos de valla para cada nodo en el clúster, así como se describe en la Sección 3.7, “Configuración de cercado para miembros de clúster”.
- Actualización de dispositivos de valla — Consulte la Sección 3.6.2, “Modificación de un dispositivo de valla”.
- Borrado de servicios de valla — Consulte la Sección 3.6.3, “Borrado de un dispositivo de valla”.

Desde la página específica de clúster, puede configurar los dispositivos de vallas para ese clúster, si hace clic en **Dispositivos de valla** en la parte superior de la pantalla de clúster. Así muestra los dispositivos de valla para el clúster y muestra los elementos de menú para configuración de dispositivos de valla: **Añadir** y **Borrar**. Este es el punto de partida de cada procedimiento descrito en las siguientes secciones.

Nota

Si se trata de una configuración de clúster inicial, no se ha creado ningún dispositivo de valla, y por lo tanto, no se muestra ninguno.

Figura 3.5, “Página de configuración de dispositivos de valla de luci ” muestra dispositivos de vallas de pantalla de configuración antes de que cualquier dispositivo de valla haya sido creado.

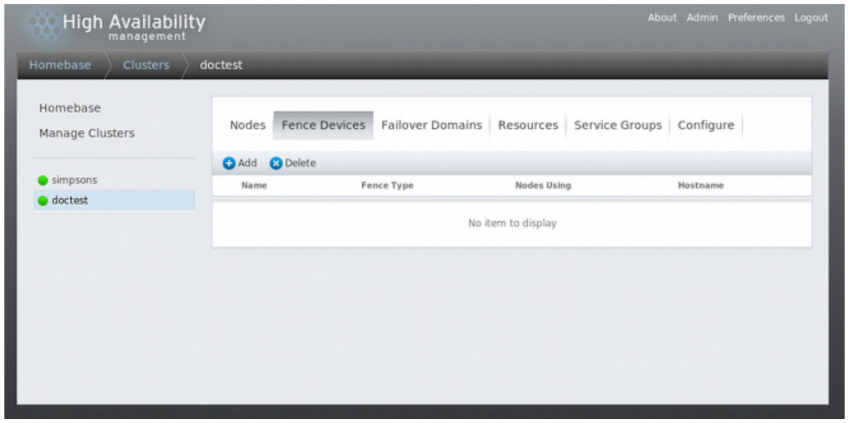

Figura 3.5. Página de configuración de dispositivos de valla de luci

3.6.1. Cómo crear un dispositivo de valla

Para crear un dispositivo de vallas, siga los siguientes pasos:

1. Desde la página de configuración **Dispositivos de valla**, haga clic en **Añadir**. Al hacer clic en **Añadir** aparece el cuadro de diálogo **Añadir dispositivo de valla (instancia)**. Desde este cuadro de diálogo, seleccione el tipo de dispositivo de valla a configurar.
2. Especifique la información en el cuadro de diálogo **Añadir un dispositivo de valla (instancia)** según el tipo de dispositivo de valla. Para obtener mayor información sobre parámetros de dispositivos de valla, consulte el Apéndice A, *Parámetros de dispositivos de valla*. En algunos casos se necesitarán especificar parámetros específicos de nodos adicionales para el dispositivo de valla al configurar el cercado para nodos individuales, como se describe en la Sección 3.7, "Configuración de cercado para miembros de clúster".
3. Haga clic en **Enviar**.

Después de añadir el dispositivo de valla, aparece en la página de configuración **Dispositivos de valla**.

3.6.2. Modificación de un dispositivo de valla

Para modificar un dispositivo de valla, siga los siguientes pasos:

1. Desde la página de configuración **Dispositivos de valla**, haga clic en el nombre de dispositivo de valla a modificar. Este muestra el cuadro de diálogo para el dispositivo de valla, con los valores que han sido configurados para el dispositivo.
2. Para modificar el dispositivo de valla, ingrese los cambios para los parámetros desplegados. Para obtener mayor información, consulte, el Apéndice A, *Parámetros de dispositivos de valla*.
3. Haga clic en **Aplicar** y espere a que la configuración se actualice.

3.6.3. Borrado de un dispositivo de valla

Nota

Los dispositivos de valla que se están utilizando no se pueden borrar. Para borrar un dispositivo de valla que un nodo esté utilizando, primero actualice la configuración de valla de nodo para cualquier nodo que utilice el dispositivo y luego borre el dispositivo.

Para borrar un dispositivo de valla, siga los siguientes pasos:

1. Desde la página de configuración de **Dispositivos de vallas**, haga clic en la casilla a la izquierda del dispositivo o dispositivos de valla para seleccionar los dispositivos a borrar.
2. Haga clic en **Borrar** y espere que la configuración se actualice. Aparece un mensaje que indica los dispositivos que se están eliminando.

Cuando se ha actualizado la configuración, el dispositivo de valla eliminado ya no aparece en la pantalla.

3.7. Configuración de cercado para miembros de clúster

Una vez que haya completado los pasos iniciales de la creación de un clúster y creación de dispositivos de valla, necesita configurar el cercado para los nodos de clúster. Para configurar el cercado para los nodos después de crear un nuevo clúster y configurar los dispositivos de cercado para el clúster, siga los pasos descritos en esta sección. Tenga en cuenta que debe configurar el cercado para cada nodo del clúster.

Las secciones siguientes proporcionan procedimientos para la configuración de un dispositivo de valla único para un nodo, la configuración de un nodo con un dispositivo de valla de copia de seguridad y la configuración de un nodo con fuentes de alimentación redundantes:

- Sección 3.7.1, "Configuración de un dispositivo de vallas único para un nodo"
- Sección 3.7.2, "Configuración de un dispositivo de vallas de respaldo"
- Sección 3.7.3, "Configuración de un nodo con energía redundante "

3.7.1. Configuración de un dispositivo de vallas único para un nodo

Siga el procedimiento a continuación para configurar un nodo con un dispositivo de vallas único.

1. Desde la página específica de clúster, puede configurar el cercado de nodos en el clúster. Haga clic en **Nodos** en la parte superior de la pantalla de clúster. Así visualizará los nodos que constituyen el clúster. También es la página predeterminada que aparece al hacer clic en el nombre de clúster debajo de **Administrar clústeres** del menú a la izquierda de **luci** en la página de **Base de origen**.
2. Haga clic en el nombre de nodo. Al hacer clic en un enlace para un nodo aparece la página para ese enlace que muestra cómo se configura ese nodo.

La página específica de nodo muestra los servicios que están actualmente ejecutándose en el nodo, así como también los dominios de conmutación de los cuales este nodo es un miembro. Puede modificar un dominio de conmutación al hacer clic en su nombre. Para obtener mayor información sobre configuración de dominios de conmutación, consulte la Sección 3.8, "Configuración de dominio de conmutación".

3. En la página específica de nodo, bajo **Dispositivos de valla**, haga clic en **`Añadir método de valla`**. Este desplegará el cuadro de diálogo **`Añadir método de valla a nodo`**.
4. Ingrese el **Nombre de método** para el método de cercado que está configurando para este nodo. Es un nombre arbitrario que será utilizado por la adición de alta disponibilidad de Red Hat. No es lo mismo que el nombre de DNS para el dispositivo.
5. Haga clic en **`Enviar`**. Así aparece una pantalla específica de nodo que ahora despliega el método que acaba de añadir bajo **Dispositivos de vallas**.
6. Configure una instancia de valla para este método al hacer clic en el botón **`Añadir una instancia de valla`**. De esta manera se muestra el menú desplegable **Añadir dispositivo de valla (Instancia)** desde el cual puede seleccionar un dispositivo de valla que anteriormente haya configurado, como se describe en la Sección 3.6.1, "Cómo crear un dispositivo de valla".
7. Seleccione un dispositivo para este método. Si el dispositivo de valla requiere que usted configure los parámetros de nodos específicos, la pantalla muestra los parámetros a configurar. Para obtener mayor información sobre parámetros de cercado, consulte el Apéndice A, *Parámetros de dispositivos de valla*.

   Nota

   Para métodos de valla sin-energía (es decir, SAN/cercado de almacenamiento), se predetermina a **Sin cercado** en la pantalla de parámetros específicos de nodos. Esto garantiza que el acceso del nodo cercado al almacenaje no se reactive, sino hasta que el nodo haya sido reiniciado. Para obtener mayor información sobre quitar la valla a un nodo, consulte la página de manual **`fence_node`**(8).

8. Haga clic en **`Enviar`**. Así lo devuelve a la pantalla de nodo específico con el método de vallas e instancia de vallas desplegada.

3.7.2. Configuración de un dispositivo de vallas de respaldo

Puede definir varios métodos de cercado para un nodo. Si el cercado falla con el primer método, el sistema intentará cercar el nodo con un segundo método, seguido de métodos adicionales que usted haya configurado.

Siga el procedimiento a continuación para configurar un dispositivo de vallas de respaldo para un nodo.

1. Siga el procedimiento provisto en la Sección 3.7.1, "Configuración de un dispositivo de vallas único para un nodo" para configurar el método de cercado primario para un nodo.
2. Debajo de la pantalla del método primario que definió, haga clic en **`Añadir un método de valla`**.
3. Ingrese el método de cercado de respaldo que usted esté configurando para este nodo y haga clic en **`Enviar`**. De esta manera, muestra la pantalla específica de nodo que ahora despliega el método que ha acabado de añadir, debajo del método de vallas primario.
4. Configure una instancia de valla para este método al hacer clic en **`Añadir una instancia de valla`**. De esta manera se muestra un menú desplegable desde el cual puede seleccionar un dispositivo de valla que anteriormente ha configurado, como se describe en la Sección 3.6.1, "Cómo crear un dispositivo de valla".
5. Seleccione un dispositivo para este método. Si el dispositivo de valla requiere que usted configure los parámetros de nodos específicos, la pantalla muestra los parámetros a configurar. Para obtener mayor información sobre parámetros de cercado, consulte el Apéndice A, *Parámetros de dispositivos de valla*.
6. Haga clic en **`Enviar`**. Así lo devuelve a la pantalla de nodo específico con el método de vallas e instancia de vallas desplegada.

Puede continuar añadiendo métodos de cercado cuando sea necesario. También puede reordenar los métodos de cercado que serán utilizados para este nodo, haciendo clic en **Subir** y **Bajar**.

3.7.3. Configuración de un nodo con energía redundante

Si el clúster se configura con fuentes de alimentación redundantes para los nodos, debe configurar el cercado para que los nodos se apaguen completamente cuando tengan que ser cercados. Si configura cada fuente alimentadora como un método de valla independiente, cada una será cercada de forma independiente; la segunda fuente de alimentación permitirá al sistema continuar

ejecutándose cuando la primera fuente de alimentación sea cercada y el sistema no será cercado por completo. Para configurar un sistema con fuentes de alimentación duales, debe configurar los dispositivos de valla para que ambas fuentes alimentadoras se apaguen y el sistema se tome completamente. Al configurar su sistema mediante **conga**, debe configurar dos instancias dentro de un método único de cercado.

A fin de configurar el cercado para un nodo de dos fuentes de energía, siga los siguientes pasos en esta sección.

1. Antes de poder configurar el cercado para un nodo con energía redundante, debe configurar cada uno de los interruptores como un dispositivo de valla para el clúster. Para obtener mayor información sobre parámetros, consulte la Sección 3.6, "Configuración de dispositivos de valla".
2. Desde la página específica de clúster, haga clic en **Nodos** en la parte superior de la pantalla del clúster. Así muestra los nodos que constituyen el clúster. Esta es también la página predeterminada que aparece cuando hace clic en el nombre de clúster debajo de **Administrar Clústeres** del ménú a la izquierda de la página **Base de origen** de **luci**.
3. Haga clic en el nombre de nodo. Al hacer clic en un enlace para un nodo aparece la página para ese enlace que muestra cómo se configura ese nodo.
4. En la página específica de nodo, haga clic en **`Añadir un método de valla`**.
5. Ingrese el nombre para el método de cercado que usted está configurando para este nodo.
6. Haga clic en **`Enviar`**. Así aparece una pantalla específica de nodo que ahora despliega el método que acaba de añadir bajo **Dispositivos de vallas**.
7. Configure la primera fuente de energía como una instancia de valla para este método, haciendo clic en **`Añadir una instancia de vallas`**. Así, muestra un menú desplegable desde el cual puede seleccionar uno de los dispositivos de cercado de energía que anteriormente ha configurado, como se describe en la Sección 3.6.1, "Cómo crear un dispositivo de valla".
8. Seleccione un de los dispositivos de vallas de energía para este método e ingrese los parámetros apropiados para este dispositivo.
9. Haga clic en **`Enviar`**. Así lo devuelve a la pantalla de nodo específico con el método de vallas e instancia de vallas desplegada.
10. Bajo el mismo método de vallas para el cual ha configurado el primer dispositivo de cercado de energía, haga clic en **`Añadir una instancia de vallas`**. De esta manera, muestra un menú desplegable desde el cual puede seleccionar el segundo dispositivo de cercado de energía que anteriormente ha configurado, como se describió en la Sección 3.6.1, "Cómo crear un dispositivo de valla".
11. Seleccione el segundo de los dispositivos de valla de energía para este método e ingrese los parámetros apropiados para este dispositivo.
12. Haga clic en **`Enviar`**. Esto lo devuelve a la pantalla específica de nodo con los métodos de valla e instancias de valla desplegadas, mostrando que cada dispositivo apagará el sistema en secuencia y encenderá el sistema en secuencias. Esto se muestra en la Figura 3.6, "Configuración de cercado de doble energía".

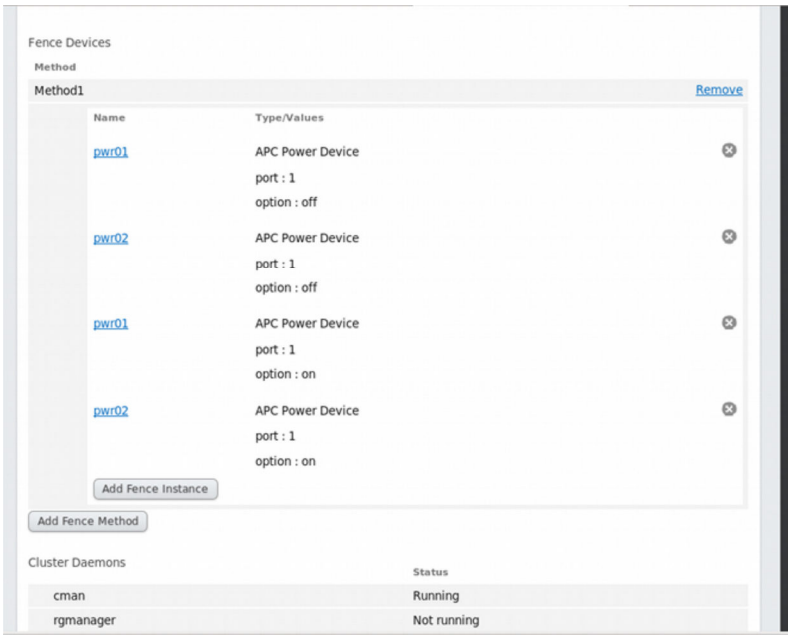

Figura 3.6. Configuración de cercado de doble energía

3.8. Configuración de dominio de conmutación

Un dominio de conmutación es un subconjunto con nombre de nodos de clúster elegibles para ejecutar un servicio de clúster en caso de una falla de nodo. Un dominio de conmutación puede tener las siguientes características:

- Sin restricciones — Le permite especificar que un subconjunto de miembros se prefiera, pero que el servicio de clúster asignado a este dominio pueda ejecutarse en cualquier miembro disponible.
- Restringido — Le permite restringir los miembros que pueden ejecutar un servicio de clúster particular. Si ninguno de los miembros en un dominio de conmutación restringido está disponible, el servicio de clúster no puede iniciarse (ya sea en forma manual o por el software de clúster).
- Desordenado — Cuando el servicio de clúster se asigna a un dominio de conmutación desordenado, el miembro en el que se ejecuta el servicio de clúster es elegido entre los miembros de dominio de conmutación sin ningún orden de prioridad.
- Ordenado — Le permite especificar un orden de preferencia entre los miembros del dominio de conmutación. El miembro en la parte superior de la lista es el preferido, seguido del segundo miembro en la lista, y así sucesivamente.
- Recuperación — Le permite especificar si un servicio en el dominio de conmutación debe recuperar al nodo que originalmente estaba ejecutándose antes de que ese nodo falle. La configuración de esta característica es útil en circunstancias donde un nodo repetidamente falla y hace parte de un dominio de conmutación ordenado. En esas circunstancias, si un nodo es el nodo preferido en un dominio de conmutación, es posible que un servicio se conmute o se recupere repetidas veces entre el nodo preferido y otro nodo, lo cual repercute gravemente en el rendimiento.

Nota

La característica de recuperación de fallos se aplica únicamente si la configuración de fallos ordenada está configurada.

Nota

El cambio de una configuración de dominio de recuperación no se efectúa en servicios que se están ejecutando.

Nota

Los dominios de conmutación *no* se requieren para operación.

Por defecto, los dominios de conmutación son desordenados y sin restricciones.

En un clúster con varios miembros, si utiliza un dominio de conmutación restringido puede minimizar la labor de configuración del clúster para ejecutar un servicio de clúster (como **`httpd`**), el cual requiere que establezca la configuración idéntica en todos los miembros que ejecuten el servicio de clúster. En lugar de configurar todo el clúster para que ejecute el servicio de clúster, únicamente configure los miembros del dominio de conmutación restringido asociados con el servicio de clúster.

Nota

Para configurar a un miembro preferido, puede crear un dominio de conmutación sin restricciones que consta de un único miembro del clúster. Al hacer esto, el servicio de clúster se ejecutará en ese miembro del clúster principalmente (el miembro preferido), pero permitirá que el servicio de clúster recupere fallas de cualquiera de los otros miembros.

Las secciones a continuación describen cómo añadir, modificar y borrar un dominio de conmutación.

- Sección 3.8.1, “Adición de un dominio de conmutación ”
- Sección 3.8.2, “Modificación de un dominio de conmutación”
- Sección 3.8.3, “Borrado de un dominio de conmutación”

3.8.1. Adición de un dominio de conmutación

Para añadir un dominio de conmutación, siga los pasos en esta sección.

1. Desde la página específica de clúster, puede configurar dominios de conmutación para ese clúster al hacer clic en **Dominios de conmutación** en la parte superior de la pantalla de clúster. Así despliega los dominios de conmutación que han sido configurados para este clúster.
2. Haga clic en **Añadir**. Al hacer clic en **Añadir** aparece la ventana de **`Añadir un dominio al clúster`**, como se muestra en la Figura 3.7, “Cuadro de diálogo de configuración de dominio de conmutación de luci”.

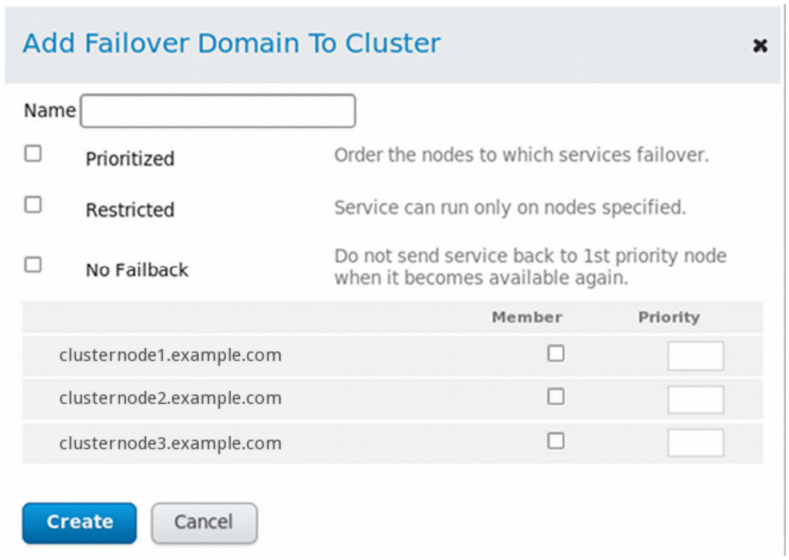

Figura 3.7. Cuadro de diálogo de configuración de dominio de conmutación de luci

3. En el cuadro de diálogo **`Añadir un dominio de conmutación al clúster`**, especifique un nombre de dominio de conmutación en la casilla de texto **Nombre**.

> **Nota**
>
> El nombre debe ser bastante descriptivo para distinguir su propósito relativo a otros nombres utilizados en su clúster.

4. Para activar la configuración de prioridad de conmutación de los miembros en el dominio de conmutación, haga clic en la casilla de verificación **Con prioridad**. Cuando haya activado **Con prioridad**, puede establecer el valor de prioridad, **Prioridad**, para cada nodo seleccionado como miembro del dominio de conmutación.
5. Para restringir a miembros en el dominio de conmutación, haga clic en la casilla de verificación **Restringido**. Cuando haya activado **Restringido**, los servicios asignados a este dominio de conmutación recuperan solamente los nodos en este dominio de conmutación.
6. Para especificar que un nodo no se recupere en este dominio de conmutación, haga clic en la casilla de verificación **Sin recuperación de fallos**. Cuando haya activado **Sin recuperación de fallos**, si el servicio se conmuta desde un nodo preferido, el servicio no se recuperará a su nodo original una vez se haya recuperado.
7. Configure los miembros para este dominio de conmutación. Haga clic en la casilla de verificación de **Miembro** para cada nodo que vaya a ser miembro del dominio de conmutación. Si marca **Con prioridad**, establezca la prioridad en la casilla de texto **Prioridad** para cada miembro de dominio de conmutación.
8. Haga clic en **`Crear`**. Así, muestra la página de **`Dominios de conmutación`** con el dominio de conmutación recién creado. Un mensaje indica que el nuevo dominio está siendo creado. Actualice la página para obtener un estatus actualizado.

3.8.2. Modificación de un dominio de conmutación

Para modificar un dominio de conmutación, siga los siguientes pasos en esta sección.

1. Desde la página específica de clúster, haga clic en **Dominios de conmutación** en la parte superior de la pantalla de clúster para configurar dominios de conmutación para ese clúster.
2. Haga clic en el nombre del dominio de conmutación. Así aparece la página de configuración para ese dominio de conmutación.
3. Para modificar las propiedades **Con prioridad**, **Restringido**, o **Sin recuperación** para el dominio de conmutación, active o desactive la casilla de verificación cerca de la propiedad y haga clic en **`Actualizar propiedades`**.
4. Pare modificar la membresía de dominio de conmutación, active o desactive la casilla de verificación cerca del miembro de clúster. Si el dominio de conmutación tiene prioridad, también puede establecer la prioridad para el miembro de clúster. Haga clic en **`Actualización de configuración`**.

3.8.3. Borrado de un dominio de conmutación

Para borrar un dominio de conmutación, siga los siguientes pasos en esta sección.

1. Desde la página específica de clúster, haga clic en **Dominios de conmutación** en la parte superior de la pantalla de clúster para configurar dominios de conmutación para ese clúster.
2. Seleccione la casilla de verificación para borrar un dominio de conmutación.
3. Haga clic en **Borrar**.

3.9. Configuración de recursos de clúster globales

Puede configurar recursos globales que pueden ser utilizados por cualquier servicio ejecutándose en un clúster y puede configurar recursos que estén disponibles solamente para un servicio específico.

Para añadir un recurso de clúster global, siga los pasos en esta sección. Puede añadir un recurso que sea local a un servicio particular cuando configure el servicio, como se describió en la Sección 3.10, “Adición de un servicio de clúster al clúster”.

1. Desde la página específica de clúster, puede añadir recursos a ese clúster haciendo clic en **Recursos** en la parte superior de la pantalla de clúster. De esta manera, muestra los recursos que han sido configurados para ese clúster.
2. Haga clic en **Añadir**. De esta manera, muestra el menú desplegable de **Añadir un recurso al clúster**.
3. Haga clic en la casilla desplegable bajo **Añadir un recurso al clúster** y seleccione el tipo de recurso a configurar.
4. Ingrese los parámetros de recursos para el recurso que está añadiendo. El Apéndice B, *Parámetros de recursos de alta disponibilidad* describe los parámetros de recursos.
5. Haga clic en **`Enviar`**. Al hacer clic en **`Enviar`** retorna a la página de recursos que muestra la pantalla de **`Recursos`**, la cual muestra los recursos añadidos (y otros más).

Para modificar un recurso existente, realice los siguientes pasos.

1. Desde la página **luci Recursos**, haga clic en el nombre del recurso a modificar. Así muestra los parámetros para ese recurso.
2. Edite los parámetros de recursos.
3. Haga clic en **`Aplicar`**.

Para borrar un recurso existente, realice los siguientes pasos.

1. Desde la página **luci Recursos**, haga clic en la casilla de verificación para borrar cualquier recurso.
2. Haga clic en **Borrar**.

3.10. Adición de un servicio de clúster al clúster

Para añadir un servicio de clúster al clúster, sigan los siguientes pasos en esta sección.

1. Desde la página específica de clúster, puede añadir servicios a ese clúster al hacer clic en **Grupos de servicios** en la parte superior de la pantalla de clúster. Así despliega los servicios que han sido configurados para ese clúster. (Desde la página **Grupos de Servicios**, puede también iniciar, reiniciar, e inhabilitar un servicio, como se describe en la Sección 4.5, “Administrar servicios de alta disponibilidad”).
2. Haga clic en **Añadir**. Así, despliega el cuadro de diálogo **Añadir un grupo de servicio al clúster**.
3. En el cuadro de diálogo **`Añadir un grupo de servicio al clúster`**, en la caja de

texto de **Nombre de servicio**, escriba el nombre del servicio.

Nota

Use un nombre descriptivo que distinga claramente el servicio de otros servicios en el clúster.

4. Marque la casilla de verificación **Automáticamente inicie este servicio** si desea que el servicio inicie automáticamente cuando un clúster se inicie y se ejecute. Si la casilla de verificación *no* se marca, el servicio debe ser iniciado de forma manual en cualquier momento que el clúster salga del estado parado.
5. Marque la casilla de verificación **Ejecutar exclusivo** para establecer una política donde el servicio solamente se ejecuta en nodos que no tienen otros servicios ejecutándose en ellos.
6. Si ha configurado los dominios de conmutación para el cluster, use el menú desplegable del parámetro **Dominio de conmutación** para seleccionar un dominio de conmutación para este servicio. Para obtener mayor información sobre cómo configurar dominios de conmutación, consulte la Sección 3.8, “Configuración de dominio de conmutación”.
7. Use la caja desplegable **Política de recuperación** para seleccionar una política de recuperación para el servicio. Las opciones son para **Reubicar**, **Reiniciar**, **Reiniciar-Inhabilitar**, o **Inhabilitar** el servicio.

   Al seleccionar la opción **Reiniciar** indica que el sistema debe intentar reiniciar el servicio que falló antes de reasignar el servicio. Si selecciona la opción **Reubicar** indica que el sistema debe intentar reiniciar el servicio en un nodo diferente. Si selecciona la opción **Inhabilitar** indica que el sistema debe desactivar el grupo de recursos si algún componente falla. Al seleccionar la opción **Reiniciar-Inhabilitar** indica que el sistema debe intentar reiniciar el servicio en su lugar si el servicio falla, pero si en el reinicio el servicio falla, el servicio se desactivará en lugar de desplazarse a otro host en el clúster.

   Si selecciona **Reiniciar** o **Reiniciar-Inhabilitar**como política de recuperación para el servicio, puede especificar el número máximo de fallas de reinicio antes de reubicar o desactivar el servicio y el tiempo en segundos después del cual olvida reiniciar.
8. Para añadir un recurso al servicio, haga clic en **`Añadir un recurso`**. Al hacer clic en **`Añadir un recurso`** se muestra una casilla desplegable **`Añadir un recurso al servicio`** que permite añadir un recurso global existente o añadir un nuevo recurso que *solamente* está disponible para este servicio.
   - Para añadir un recurso global, haga clic en el nombre del recurso existente desde la casilla desplegable **`Añadir un recurso a este servicio`**. De esta manera muestra el recurso y sus parámetros en la página **Grupos de servicios** para el servicio que usted está configurando. Para obtener mayor información sobre adición y modificación de recursos globales, consulte la Sección 3.9, “Configuración de recursos de clúster globales”).
   - Para añadir un nuevo recurso que esté disponible únicamente para este servicio, seleccione el tipo de recursos a configurar desde la casilla desplegable de **`Añadir un recurso al servicio`** e ingrese los parámetros de recursos para el recurso que usted está añadiendo. Apéndice B, *Parámetros de recursos de alta disponibilidad* describe los parámetros de recursos.
   - Al añadir un recurso al servicio, ya sea un recurso global existente o un recurso disponible solamente para este servicio, puede especificar si el recurso es un **Subárbol independente** o un **Recurso no crítico**.

     Si especifica que ese un recurso es un subárbol independiente, entonces si ese recurso falla solo se reiniciará ese recurso antes de que el sistema intente la recuperación normal. Puede especificar el número máximo de reinicios para intentar en un nodo antes de implementar la política de recuperación para ese servicio. También puede especificar el tiempo en segundos después del cual el sistema implementará la política de recuperación para el servicio.

     Si especifica el recurso como no-crítico, entonces si ese recurso falla únicamente ese recurso se reiniciará y si el recurso sigue fallando entonces solamente ese recurso se inhabilitará, en lugar de todo el servicio. Puede especificar un número máximo de reinicios para intentar especificar el tiempo en segundos después del cual se desactivará el recurso.
9. Si desea añadir recursos de hijo al recurso que usted está definiendo, haga clic en **`Añadir un recurso hijo`**. Al hacer clic en **`Añadir un recurso hijo`** se despliega la pantalla de la cajilla desplegable **Añadir un recurso al servicio**, desde la cual puede añadir un recurso global existente o añadir un nuevo recurso que esté disponible únicamente para este servicio. Puede continuar añadiendo recursos de hijos al recurso para ajustar sus requerimientos.

Nota

Si está añadiendo un recurso de servicio Samba, añádalo directamente al servicio, *no* como un hijo de otro recurso.

10. Cuando haya terminado de añadir recursos al servicio y de añadir recursos de hijos a recursos, haga clic en **Enviar**. Al hacer clic en **Enviar** vuelve a la página de **Grupos de servicios** que muestra el servicio añadido (y otros servicios).

Nota

Para verificar la existencia del recurso de servicios IP utilizado en un servicio de clúster, utilice el comando **/sbin/ip addr show** en un nodo de clúster (en lugar del comando obsoleto **ifconfig**). La siguiente salida muestra el comando **/sbin/ip addr show** ejecutado en un nodo que ejecuta un servicio de clúster:

```
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1356 qdisc pfifo_fast qlen 1000
    link/ether 00:05:5d:9a:d8:91 brd ff:ff:ff:ff:ff:ff
    inet 10.11.4.31/22 brd 10.11.7.255 scope global eth0
    inet6 fe80::205:5dff:fe9a:d891/64 scope link
    inet 10.11.4.240/22 scope global secondary eth0
       valid_lft forever preferred_lft forever
```

Para modificar un servicio existente, realice los siguientes pasos:

1. Desde la página de **Grupos de servicios**, haga clic en el nombre del servicio a modificar. Así muestra los parámetros y recursos que han sido configurados para ese servicio.
2. Edite los parámetros de servicios.
3. Haga clic en **Enviar**.

Para borrar uno o más servicios existentes, realice los siguientes pasos.

1. Desde la página **luci Grupo de servicios**, haga clic en la casilla de verificación para borrar cualquier servicio.
2. Haga clic en **Borrar**.
3. A partir del lanzamiento de Red Hat Enterprise Linux 6.3, antes de que **luci** borre los servicios, aparecerá un mensaje preguntándole si desea confirmar su intención de borrar los grupos de servicios o grupos, lo cual detiene los recursos que lo comprenden. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin borrar ningún servicio, o haga clic en **Proseguir** para retirar el servicio o los servicios seleccionados.

Capítulo 4. Administración de adición de alta disponibilidad de Red Hat con Conga

4.1. Añadir un clúster existente a la interfaz luci

4.2. Retirar un clúster existente a la interfaz luci

4.3. Administrar nodos de clúster
- 4.3.1. Reinicio de un nodo de clúster
- 4.3.2. Hacer que un nodo abandone o se una a un clúster
- 4.3.3. Añadir un miembro a un clúster en ejecución
- 4.3.4. Borrado de un miembro de un clúster

4.4. Iniciar, parar, reiniciar, y borrar clústeres

4.5. Administrar servicios de alta disponibilidad

4.6. Cómo hacer una copia de seguridad y restaurar la configuración de luci

Este capítulo describe varias tareas administrativas para el manejo de adición de alta disponibilidad de Red Hat y consta de las siguientes secciones:

- Sección 4.1, “Añadir un clúster existente a la interfaz luci”
- Sección 4.2, “Retirar un clúster existente a la interfaz luci”
- Sección 4.3, “Administrar nodos de clúster”
- Sección 4.4, “Iniciar, parar, reiniciar, y borrar clústeres”
- Sección 4.5, “Administrar servicios de alta disponibilidad”
- Sección 4.6, “Cómo hacer una copia de seguridad y restaurar la configuración de luci”

4.1. Añadir un clúster existente a la interfaz luci

Si anteriormente creó un clúster de adición de alta disponibilidad, puede fácilmente añadir el clúster a la interfaz **luci** para poder manejar el clúster con **Conga**.

Para añadir un clúster existente a la interfaz **luci**, siga los siguientes pasos:

1. Al hacer clic en **Administrar clúster** desde el menú en la parte izquierda de la página de **luci Homebase**. Aparecerá la pantalla de **clústeres**.
2. Al hacer clic en **Añadir**, aparecerá la pantalla **Añadir un clúster existente**.
3. Ingrese el nombre de host de nodo y la contraseña de **ricci** para cualquiera de los nodos en el clúster existente. Puesto que cada nodo en el clúster contiene toda la información para el clúster, se debe proporcionar suficiente información para añadir el clúster a la interfaz de **luci**.
4. Al hacer clic en **`Conectar`**, aparecerá la pantalla **Añadir un clúster existente** luego aparecerá el nombre de clúster y los nodos restantes en el clúster.
5. Ingrese las contraseñas individuales de **ricci** para cada nodo en el clúster, o ingrese una contraseña y seleccione **Usar la misma contraseña para todos los nodos**.
6. Haga clic en **`Añadir clúster`**. El clúster anteriormente configurado ahora se muestra en la pantalla **Administrar clúster**.

4.2. Retirar un clúster existente a la interfaz luci

Puede retirar un clúster de la Interfaz gráfica de usuario de administración de **luci** sin afectar los servicios o membresía de clúster. Si retira un clúster, puede más adelante volverlo a anadir o añadirlo a otra instancia de **luci**, como se describen en la Sección 4.1, “Añadir un clúster existente a la interfaz luci”.

Para añadir un clúster de la interfaz de usuario de administración de **luci** sin afectar los servicios o membresía de clúster, siga los siguientes pasos:

1. Al hacer clic en **Administrar clúster** desde el menú en la parte izquierda de la página de **luci Homebase**. Aparecerá la pantalla de **clústeres**.
2. Seleccione el clúster o los clústeres que desea retirar.
3. Haga clic en **Borrar**.

Para obtener información sobre borrar completamente un clúster, detener todos los servicios de clúster, retirar la información de configuración de clúster de los propios nodos, consulte la Sección 4.4, “Iniciar, parar, reiniciar, y borrar clústeres”.

4.3. Administrar nodos de clúster

Esta sección documenta cómo realizar las siguientes funciones de administración de nodos a través del componente del servidor **luci** de **Conga**:

- Sección 4.3.1, “Reinicio de un nodo de clúster”
- Sección 4.3.2, “Hacer que un nodo abandone o se una a un clúster”
- Sección 4.3.3, “Añadir un miembro a un clúster en ejecución”
- Sección 4.3.4, “Borrado de un miembro de un clúster”

4.3.1. Reinicio de un nodo de clúster

Para reiniciar un nodo en un clúster, realice los siguientes pasos:

1. Desde la página específica de clúster, haga clic en **Nodos** en la parte superior de la pantalla del clúster. Así muestra los nodos que constituyen el clúster. También es la página predeterminada que aparece cuando hace clic en el nombre de clúster bajo **Administrar clúster** del menú a la izquierda de la página de **luci Homebase**.
2. Haga clic en la casilla de verificación del nodo a reiniciar.
3. Seleccione la función **Reiniciar** desde el menú en la parte superior de la página. Así, el nodo seleccionado reinicia y aparece un mensaje en la parte superior de la página que el nodo está reiniciando.
4. Actualice la página para ver el estatus actualizado del nodo.

Es posible reiniciar más de un nodo al mismo tiempo si selecciona todos los nodos que desea reiniciar antes de hacer clic en **Reiniciar**.

4.3.2. Hacer que un nodo abandone o se una a un clúster

Puede usar el componente del servidor **luci** de **Conga** para hacer que el nodo abandone un clúster activo parando todos los servicios de clúster en el nodo. Puede también usar el componente de servidor **luci** de **Conga** para hacer que un nodo que ha abandonado un clúster se reúna al clúster.

Al hacer que el nodo abandone un clúster no se elimina la información de configuración de clúster de ese nodo, y el nodo aún aparece en la pantalla de nodo de clúster con un estatus de **`No miembro de clúster`**. Para obtener mayor información sobre borrado total de la configuración de clúster, consulte la Sección 4.3.4, “Borrado de un miembro de un clúster”.

Para hacer que un nodo abandone un clúster, realice los siguientes pasos. Así, cierra el software de clúster en el Nodo. Al hacer que el nodo abandone el clúster evita que el nodo automáticamente se una al clúster en el reinicio.

1. Desde la página específica de clúster, haga clic en **Nodos** en la parte superior de la pantalla del clúster. Así muestra los nodos que constituyen el clúster. También es la página predeterminada que aparece cuando hace clic en el nombre de clúster bajo **Administrar clúster** del menú a la izquierda de la página de **luci Homebase**.
2. Haga clic en la casilla de verificación del nodo que desea abandonar el clúster.
3. Seleccione la función **Abandonar clúster** desde el menú en la parte superior de la página. Esto hace que aparezca un mensaje en la parte superior de la página indicando que el nodo está siendo detenido.
4. Actualice la página para ver el estatus actualizado del nodo.

También es posible hacer que más de un nodo abandone el clúster al seleccionar todos los nodos para que abandonen el clúster antes de hacer clic en **Abandonar clúster**.

Para que un nodo se reúna con un clúster, seleccione los nodos que desee reunir al clúster haciendo clic en la casilla de verificación para esos nodo y seleccione **Unir clúster**. Esto hace que los nodos seleccionado se unan al clúster y permite que los nodos seleccionado se unan al clúster al reinicio.

4.3.3. Añadir un miembro a un clúster en ejecución

Para añadir a un miembro que esté ejecutando clúster , siga los siguientes pasos en esta sección.

1. Desde la página específica de clúster, haga clic en **Nodos** en la parte superior de la pantalla de clúster. Así muestra los nodos que constituyen el clúster. También es la página predeterminada que aparece cuando hace clic en el nombre del clúster debajo de **Administrar clústeres** desde el menú a la izquierda de la página de **luciHomebase**.
2. Haga clic en **Añadir**. Al hacer clic en **Añadir** se muestra la ventana de diálogo **`Añadir nodos al clúster`**.

3. Ingrese el nombre de nodo en la cajilla de texto **Nombre de host de nodo** e ingrese la contraseña de **ricci** en la cajilla de texto de **Contraseña**. Si está utilizando un puerto para el agente **ricci**, diferente al predeterminado 11111, puede cambiar ese parámetro al puerto que está utilizando.
4. Seleccione **Habilitar el soporte de almacenamiento compartido** si el almacenamiento en clúster se requiere para descargar los paquetes que soportan almacenamiento en clúster y activar LVM en clúster. Debe seleccionarlo solamente cuando tenga acceso a la adición de almacenamiento resistente o a la adición del sistema de archivos escalable.
5. Si desea añadir más nodos, haga clic en **`Añadir otro nodo`** e ingrese el nombre de nodo y contraseña para cada nodo adicional.
6. Haga clic en **`Añadir nodos`**. Al hacer clic en **`Añadir nodos`** se produce lo siguiente:
   a. Si ha seleccionado **Descargar paquetes**, los paquetes de software de clúster se descargarán en los nodos.
   b. El software de clúster se instala en los nodos (o se verifica que los paquetes de software instalados sean apropiados).
   c. El archivo de configuración de clúster se actualiza y propaga para cada nodo en el clúster — incluyendo el nodo añadido.
   d. El nodo añadido se une al clúster.

   La página **Nodos** aparece con un mensaje indicando que el nodo está siendo utilizado para el clúster. Actualice la página para actualizar el estatus.
7. Cuando el proceso de añadir un nodo se complete, haga clic en el nombre de nodo para el nodo recién añadido a fin de configurar vallas para este nodo, como se describe en la Sección 3.6, “Configuración de dispositivos de valla”.

4.3.4. Borrado de un miembro de un clúster

Para borrar a un miembro de un clúster existente que esté ejecutándose, siga los siguientes pasos en esta sección. Observe que los nodos deben detenerse antes de ser borrados a menos que borre todos los nodos en el clúster a la vez.

1. Desde la página específica de clúster, haga clic en **Nodos** en la parte superior de la pantalla de clúster. Así muestra los nodos que constituyen el clúster. También es la página predeterminada que aparece cuando hace clic en el nombre del clúster debajo de **Administrar clústeres** desde el menú a la izquierda de la página de **luciHomebase**.

   Nota

   Para permitir que los servicios que se ejecutan en un nodo se conmuten cuando se elimine el nodo, ignore este paso.

2. Inhabilitar o reubicar cada servicio que esté ejecutándose en el nodo que va a ser borrado. Para obtener información sobre cómo desactivar y reubicar servicios, consulte la Sección 4.5, “Administrar servicios de alta disponibilidad”.
3. Seleccione el nodo o nodos a borrar.
4. Haga clic en **Borrar**. La página de **`Nodos`** indica que el nodo está siendo eliminado. Actualice la página para ver el estatus actual.

Importante

El retiro de un nodo de clúster del clúster es una operación destructiva que no puede deshacerse.

4.4. Iniciar, parar, reiniciar, y borrar clústeres

Puede iniciar, parar o reiniciar un clúster al realizar estas acciones en los nodos individuales en el clúster. Desde la página específica de clúster, haga clic en **Nodos** a lo largo de la pantalla de clúster. Así muestra los nodos que constituyen el clúster.

El inicio y reinicio de operaciones para nodos de clúster o un clúster completo, cree cortes de un servicio de clúster cortos si un servicio de clúster necesita ser trasladado a otro miembro de clúster debido a que está ejecutándose en un nodo que está deteniéndose o reiniciando.

Si desea parar un clúster, siga los siguientes pasos. Esto apaga el software de clúster en los nodos, pero no retira la información de configuración de clúster desde los nodos y los nodos aún aparecen en la pantalla de el nodo de clúster con un estatus de **`No miembro de clúster`**.

1. Haga clic en la cajilla de verificación cerca de cada nodo para seleccionar todos los nodos en

el clúster.

2. Seleccione la función **Abandonar clúster** desde el menú en la parte superior de la página. Así, el mensaje aparece en la parte superior de la página indicando que se ha detenido cada nodo.
3. Actualice la página para ver el estatus actualizado de los nodos.

Para iniciar un clúster, realice los siguientes pasos:

1. Haga clic en la cajilla de verificación cerca de cada nodo para seleccionar todos los nodos en el clúster.
2. Seleccione la función **Unir a un clúster** desde el menú en la parte superior de la página.
3. Actualice la página para ver el estatus actualizado de los nodos.

Para reiniciar un clúster en ejecución, detenga primero todos los nodos en el clúster, luego inicie todos los nodos en el clúster, como se describió arriba.

Para borrar completamente un clúster, realice los siguientes pasos. Esto hace que todos los servicios de clúster detengan y retiren la información de los propios nodos y los retire de la pantalla de clúster. Si más adelante trata de añadir un clúster existente mediante el uso de nodos que haya borrado, **luci** indicará que el nodo no es miembro de ningún clúster.

Importante

Borrar un clúster es una operación destructora que no se puede revertir. Para restaurar un clúster después de haberlo borrado se requiere que usted cree y redefina el clúster desde el comienzo.

1. Haga clic en la cajilla de verificación cerca de cada nodo para seleccionar todos los nodos en el clúster.
2. Seleccione la función **Borrar** desde el menú en la parte superior de la página.

Si desea retirar un clúster de la interfaz **luci** sin detener ningún servicio de clúster o membresía de clúster, puede usar la opción **Retirar** en la página **Administrar clústeres**, como se describe en la Sección 4.2, “Retirar un clúster existente a la interfaz luci”.

4.5. Administrar servicios de alta disponibilidad

Además de adicionar y modificar un servicio, como se describe en la Sección 3.10, “Adición de un servicio de clúster al clúster”, puede realizar las siguientes funciones administrativas para servicios de alta disponibilidad a través del componente del servidor **luci** de **Conga**:

- Iniciar un servicio
- Reiniciar un servicio
- Inhabilitar un servicio
- Borrar un servicio
- Reubicar un servicio

Desde la página específica de clúster, puede administrar servicios para ese clúster haciendo clic en **Grupos de servicios** en la parte superior de la pantalla de clúster. Así muestra los servicios que han sido configurados para ese clúster.

- **Iniciar un servicio** — Para iniciar un servicio que no se esté ejecutando, seleccione en la cajilla de verificación el servicio que desee iniciar y haga clic en **Iniciar**.
- **Reiniciar un servicio** — Para reiniciar un servicio que se esté ejecutando, seleccione los servicios que desea reiniciar para ese servicio y haga clic en **Reiniciar**.
- **Inhabilitar un servicio** — Para inhabilitar cualquier servicio que está actualmente en ejecución, seleccione en la casilla de verificación el servicio que desea inhabilitar para ese servicio y haga clic en **Inhabilitar**.
- **Borrar un servicio** — Para borrar un servicio que no está ejecutándose actualmente, seleccione en la casilla de verificación el servicio que desea desactivar para ese servicio y haga clic en **Borrar**.
- **Reubicar un servicio** — Para reubicar un servicio en ejecución, haga clic en el nombre del servicio en la pantalla de servicios. Esto hace que la página de configuración de servicios para el servicio que mostró, con una pantalla muestre la página de configuración de servicios para el servicio, con una pantalla indicando el nodo en que se está ejecutando el servicio.

Desde la casilla desplegable de **Iniciar en nodo...**, seleccione el nodo en el cual desea reiniciar el servicio y haga clic en el icono **Iniciar**. Un mensaje aparece en la parte superior de la pantalla indicando que el servicio se ha iniciado. Debe actualizar la pantalla para ver la nueva pantalla indicando que el servicio está ejecutándose en el nodo que ha seleccionado.

Nota

Si el servicio que está ejecutando es un servicio de **vm**, la cajilla desplegable mostrará una opción **migrate** en lugar de una opción **relocate**.

Nota

También puede reiniciar un servicio individual si hace clic en el nombre del servicio en la página de **Servicios**. Así, aparecerá la página de configuración del servicio. En la parte superior izquierda de la página de configuración del servicio están los mismos iconos para **Iniciar**, **Reiniciar**, **Inhabilitar** y **Borrar**.

4.6. Cómo hacer una copia de seguridad y restaurar la configuración de luci

A partir del lanzamiento de Red Hat Enterprise Linux 6.2, usted puede usar el siguiente procedimiento para hacer una copia de seguridad de la base de datos de **luci**, la cual se almacena en el archivo **/var/lib/luci/data/luci.db**. Esta no es la configuración de cluster que se almacena en el archivo **cluster.conf**. En su lugar, contiene la lista de usuarios, clústeres y propiedades relacionadas que **luci** mantiene. Por defecto, la copia de seguridad que se crea, será escrita en el mismo directorio como el archivo **luci.db** .

1. Ejecute **service luci stop**.
2. Ejecute **service luci backup-db**.

   También, puede especificar un nombre de archivo como un parámetro para el comando **backup-db**, el cual escribirá la base de datos **luci** a ese archivo. Por ejemplo, escriba la base de archivos de **luci** al archivo **/root/luci.db.backup**, ejecute el comando **service luci backup-db /root/luci.db.backup**. Observe que los archivos de respaldo que se escriben en sitios diferentes a **/var/lib/luci/data/** (para copias de seguridad cuyos nombres de archivos especifique cuando use **service luci backup-db**) no aparecerán en la salida del comando **list-backups**.
3. Ejecute **service luci start**.

Use el siguiente procedimiento para restaurar una base de datos de **luci**.

1. Ejecute **service luci stop**.
2. Ejecute **service luci list-backups** y observe el nombre de archivo a restaurar.
3. Ejecute **service luci restore-db /var/lib/luci/data/*lucibackupfile*** donde ***lucibackupfile*** es el archivo de respaldo a restaurar.

   Por ejemplo, el siguiente comando restaura la información de configuración de **luci** que estaba almacenada en el archivo de respaldo **luci-backup20110923062526.db**:

   ```
   service luci restore-db /var/lib/luci/data/luci-backup20110923062526.db
   ```

4. Ejecute **service luci start**.

Si necesita restaurar la base de datos de **luci**, pero ha perdido el archivo **host.pem** de la máquina en que usted creó la copia de seguridad debido a una reinstalación completa, por ejemplo, necesitará añadir otra vez de forma manual sus clústeres a **luci** para reautenticar los nodos de clúster.

Use el siguiente procedimiento para restaurar una base de datos de **luci** en otra máquina diferente a en la que se hizo la copia de seguridad. Observe que además de restaurar la base de datos misma, también necesitará copiar el archivo de certificado SSL para asegurarse que **luci** ha sido autenticada para los nodos de **ricci**. En este ejemplo, la copia de seguridad se crea en la máquina **luci1** y la copia de seguridad se restaura en la máquina **luci2**.

1. Ejecute la siguiente secuencia de comandos para crear una copia de seguridad de **luci** en **luci1** y una copia del archivo de certificado SSL y la copia de seguridad de and **luci** en **luci2**.

```
[root@luci1 ~]# service luci stop
[root@luci1 ~]# service luci backup-db
[root@luci1 ~]# service luci list-backups
/var/lib/luci/data/luci-backup20120504134051.db
[root@luci1 ~]# scp /var/lib/luci/certs/host.pem /var/lib/luci/data/luci-
backup20120504134051.db root@luci2:
```

2. En la máquina `luci2` asegúrese de que **luci** haya sido instalada y no esté en ejecución. Instale el paquete si no todavía no está instalado todavía.
3. Ejecute la siguiente secuencia de comandos para asegurarse que las auteticaciones estén en su lugar y para restaurar la base de datos de **luci** de `luci1` a `luci2`.

```
[root@luci2 ~]# cp host.pem /var/lib/luci/certs/
[root@luci2 ~]# chown luci: /var/lib/luci/certs/host.pem
[root@luci2 ~]# /etc/init.d/luci restore-db ~/luci-backup20120504134051.db
[root@luci2 ~]# shred -u ~/host.pem ~/luci-backup20120504134051.db
[root@luci2 ~]# service luci start
```

Capítulo 5. Configuración de adición de alta disponibilidad de Red Hat con el comando ccs

5.1. Visión general operativa
5.1.1. Cómo crear un archivo de configuración de clúster en un sistema local
5.1.2. Cómo ver la configuración de clúster actual
5.1.3. Cómo especificar contraseñas ricci con el comando ccs
5.1.4. Cómo modificar componentes de configuración de clúster
5.1.5. Comandos que sobrescriben los parámetros anteriores
5.1.6. Validación de configuración

5.2. Tareas de configuración

5.3. Cómo iniciar ricci

5.4. Cómo crear un clúster

5.5. Cómo configurar dispositivos de valla

5.6. Cómo listar dispositivos de vallas y opciones de dispositivos de vallas

5.7. Cómo configurar cercado para miembros de clúster
5.7.1. Cómo configurar un dispositivo de valla basado en energía simple para un nodo
5.7.2. Cómo configurar un dispositivo de valla basado en almacenamiento simple para un nodo
5.7.3. Cómo configurar un dispositivo de valla de respaldo
5.7.4. Cómo configurar un nodo con energía redundante
5.7.5. Cómo retirar métodos de valla e instancias de valla

5.8. Cómo configurar un dominio de conmutación

5.9. Cómo configurar recursos de clúster global

5.10. Adición de un servicio de clúster al clúster

5.11. Listado de cluster disponibles

5.12. Recursos de máquinas virtuales

5.13. Cómo configurar un disco de cuórum

5.14. Varios de configuración de clúster
5.14.1. Versión de configuración de clúster
5.14.2. Configuración de multidifusión
5.14.3. Cómo configurar un clúster de dos nodos
5.14.4. Registro
5.14.5. Cómo configurar el protocolo de anillo redundante

5.15. Cómo propagar el archivo de configuración a los nodos de clúster

A partir del lanzamiento de Red Hat Enterprise Linux 6.1, la adición de alta disponibilidad de Red Hat proporciona soporte para el comando de configuración de clúster **ccs**. El comando **ccs** permite al administrador crear, modificar, y ver el archivo de configuración de clúster **cluster.conf**. Puede usar el comando **ccs** para configurar un archivo de configuración de clúster en un sistema de archivos local o un nodo remoto. Un administrador también puede iniciar o detener los servicios de clúster con **ccs** en uno o todos los nodos en un clúster configurado.

Este capítulo describe cómo configurar el archivo de configuración de adición de alta disponibilidad de Red Hat mediante el comando **ccs**. Para obtener información sobre el uso del comando **ccs** para administrar un clúster, consulte el Capítulo 6, *Administración de adición de alta disponibilidad de Red Hat con **ccs***.

Este capítulo consta de las siguientes secciones:

- Sección 5.1, “Visión general operativa”
- Sección 5.2, “Tareas de configuración”
- Sección 5.3, “Cómo iniciar **ricci**”
- Sección 5.4, “Cómo crear un clúster”
- Sección 5.5, “Cómo configurar dispositivos de valla”
- Sección 5.7, “Cómo configurar cercado para miembros de clúster”
- Sección 5.8, “Cómo configurar un dominio de conmutación”
- Sección 5.9, “Cómo configurar recursos de clúster global”
- Sección 5.10, “Adición de un servicio de clúster al clúster”

- Sección 5.13, “Cómo configurar un disco de cuórum”
- Sección 5.14, “Varios de configuración de clúster”
- Sección 5.14, “Varios de configuración de clúster”
- Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”

Importante

Asegúrese de que su adición de alta disponibilidad cumpla con sus necesidades y tenga soporte. Consulte a un representante autorizado de Red Hat para verificar su configuración antes de ejecutarla. Además, deje un tiempo de periodo de prueba para ensayar los modos de falla.

Importante

Este capítulo hace referencia a los elementos y atributos de **cluster.conf** más utilizados. Para obtener una lista y descripción completa de **cluster.conf**, consulte el esquema de clústeren **/usr/share/cluster/cluster.rng**, y el esquema anotado en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (por ejemplo, **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

5.1. Visión general operativa

Esta sección describe los aspectos generales del uso del comando **ccs** para configurar un clúster:

- Sección 5.1.1, “Cómo crear un archivo de configuración de clúster en un sistema local”
- Sección 5.1.2, “Cómo ver la configuración de clúster actual”
- Sección 5.1.3, “Cómo especificar contraseñas ricci con el comando ccs”
- Sección 5.1.4, “Cómo modificar componentes de configuración de clúster”

5.1.1. Cómo crear un archivo de configuración de clúster en un sistema local

Para usar el comando **ccs**, puede crear un archivo de configuración de clúster en un nodo de clúster o puede crear un archivo de configuración de clúster en un sistema de archivos local y luego enviar ese archivo al host en un clúster. Esto le permite trabajar en un archivo desde una máquina local en donde puede mantenerlo bajo control de versión o de otra forma etiquetarlo de acuerdo con sus necesidades. El uso del comando **ccs** no requiere privilegios de root.

Al crear y editar un archivo de configuración de clúster en un nodo de clúster con el comando **ccs**, use la opción **-h** para especificar el nombre del host. Así crea y edita el archivo **cluster.conf** en el host:

```
ccs -h host [opciones]
```

Para crear y editar un archivo de configuración de clúster en un sistema local, use la opción **-f** del comando **ccs** para especificar el nombre del archivo de configuración al realizar una operación de clúster. Puede nombrar este archivo como lo desee.

```
ccs -f file [opciones]
```

Después de haber creado localmente el archivo, puede enviarlo al nodo del clúster mediante la opción **--setconf** del comando **ccs**. En una máquina de host en un clúster, el archivo que usted envíe se denominará **cluster.conf** y será situado en el directorio **/etc/cluster**.

```
ccs -h host -f archivo --setconf
```

Para obtener mayor información sobre el uso de la opción **--setconf** del comando **ccs**, consulte la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

5.1.2. Cómo ver la configuración de clúster actual

Si en algún momento de la creación de un archivo de configuración de clúster, desea imprimir el archivo actual, use el siguiente comando, y especifique el nodo en el clúster como host:

```
ccs -h host --getconf
```

Si está creando su archivo de configuración de clúster en un sistema local puede especificar la opción **-f** en lugar de la opción **-h** , como se describión en la Sección 5.1.1, “Cómo crear un

archivo de configuración de clúster en un sistema local".

5.1.3. Cómo especificar contraseñas ricci con el comando ccs

La ejecución de comandos **ccs** que distribuyen copias del archivo **cluster.conf** a los nodos de un clúster requiere que **ricci** esté instalado y en ejecución en los nodos del clúster, tal como se describió en la Sección 2.13, "Consideraciones para **ricci**". Para usar **ricci** requiere una contraseña la primera vez que interactúe con **ricci** desde una determinada máquina .

SI ha ingresado una contraseña para una instancia de **ricci** en una determinada máquina que usted esté utilizando, se le solicitará una contraseña cuando el comando **ccs** lo requiera. Igualmente, puede usar la opción **-p** para especificar una contraseña de **ricci** en la línea de comandos.

```
ccs -h host -p password --sync --activate
```

Cuando propaga el archivo **cluster.conf** a todos los nodos en el clúster con la opción **--sync** del comando **ccs** y especifica una contraseña para **ricci** para el comando, el comando **ccs** usará esa contraseña para cada nodo en el clúster.\n Si necesita establecer diferentes contraseñas para **ricci** en nodos individuales, puede usar la opción **--setconf** con la opción **-p** para distribuir el archivo de configuración a un nodo a la vez.

5.1.4. Cómo modificar componentes de configuración de clúster

Use el comando **ccs** para configurar componentes de clúster y sus atributos en el archivo de configuración de clúster. Tras agregar el componente de clúster al archivo, con el fin de modificar los atributos de ese componente debe retirar el componente que ha definido y añadir el componente de nuevo con los atributos modificados. Encontrará información sobre cómo hacer esto con cada componente en las secciones individuales de este capítulo.

Los atributos del componente de clúster **cman** proporcionan una excepción a este procedimiento para modificar los componentes de clúster. Para modificar dichos atributos, ejecute la opción **--setcman** del comando **ccs**, especificando los nuevos atributos. Observe que esta opción restablece todos los valores que usted no especifica explícitamente como predeterminados, así como se describe en la Sección 5.1.5, "Comandos que sobrescriben los parámetros anteriores".

5.1.5. Comandos que sobrescriben los parámetros anteriores

Hay varias opciones del comando **ccs** que implementan la semántica de sobrescritura al configurar las propiedades. Es decir, que usted puede emitir el comando **ccs** con una de estas opciones sin especificar ningún parámetro y restablecerá todos los parámetros a sus valores predeterminados. Estas opciones son las siguientes:

- **--settotem**
- **--setdlm**
- **--setrm**
- **--setcman**
- **--setmulticast**
- **--setaltmulticast**
- **--setfencedaemon**
- **--setlogging**
- **--setquorumd**

Por ejemplo, para restablecer todas las propiedadaes de demonios de vallas, puede ejecutar el siguiente comando:

```
# ccs -h hostname --setfencedaemon
```

Observe, sin embargo, que si usted usa uno de estos comandos para restablecer una propiedad, entonces las otras propiedades del comando se restablecerán a sus valores predeterminados. Por ejemplo, puede utilizar el siguiente comando para establecer la propiedad de **post_fail_delay** a 5:

```
# ccs -h hostname --setfencedaemon post_fail_delay=5
```

Si después de ejecutar ese comando, usted ejecuta el siguiente comando para restablecer la propiedad de **post_join_delay** a 10, la propiedad de **post_fail_delay** se restaurará su valor predeterminado:

```
# ccs -h hostname --setfencedaemon post_join_delay=10
```

Para restablecer las propiedades **post_fail_delay** y **post_join_delay**, indíquelas en el mismo comando, como en el siguiente ejemplo:

```
# ccs -h hostname --setfencedaemon post_fail_delay=5 post_join_delay=10
```

Para obtener mayor información sobre configuración de dispositivos de valla, consulte la Sección 5.5, “Cómo configurar dispositivos de valla”.

5.1.6. Validación de configuración

Cuando use el comando **ccs** para crear y modificar el archivo de configuración de clúster, la configuración se valida automáticamente según el esquema del clúster. A partir del lanzamiento de Red Hat Enterprise Linux 6.3, el comando **ccs** valida la configuración según el esquema de clúster en **/usr/share/cluster/cluster.rng** en el nodo que usted especifique con la opción **-h**. Anteriormente el comando **ccs** utilizaba el esquema que era empaquetado con el mismo comando **ccs**, **/usr/share/ccs/cluster.rng** en el sistema local. Si usa la opción **-f** para especificar el sistema local, el comando **ccs** aún usará el esquema de clúster **/usr/share/ccs/cluster.rng** que fue empaquetado con el propio comando **ccs** en ese sistema.

5.2. Tareas de configuración

Cómo configurar software de adición de alta disponibilidad de Red Hat con **ccs** consta de los siguientes pasos:

1. Cómo asegurarse que **ricci** está ejecutándose en todos los nodos en el clúster. Consulte la Sección 5.3, “Cómo iniciar **ricci**”.
2. Cómo crear un clúster. Consulte la Sección 5.4, “Cómo crear un clúster”.
3. Cómo configurar dispositivos de valla. Consulte la Sección 5.5, “Cómo configurar dispositivos de valla”.
4. Configuración de cercado para miembros de clúster. Consulte la Sección 5.7, “Cómo configurar cercado para miembros de clúster”.
5. Cómo crear dominios de conmutación. Consulte la Sección 5.8, “Cómo configurar un dominio de conmutación”.
6. Cómo crear recursos. Consulte la Sección 5.9, “Cómo configurar recursos de clúster global”.
7. Cómo crear servicios de clúster. Consulte la Sección 5.10, “Adición de un servicio de clúster al clúster”.
8. Cómo configurar un disco de cuórum, si es necesario. Consulte la Sección 5.13, “Cómo configurar un disco de cuórum”.
9. Cómo configurar propiedades de clúster global. Consulte la Sección 5.14, “Varios de configuración de clúster”.
10. Cómo propagar el archivo de configuración de clúster para todos los nodos de clúster. Consulte la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

5.3. Cómo iniciar ricci

Para crear y distribuir archivos de configuración en los nodos del clúster, el servicio **ricci** debe estar ejecutándose en cada nodo. Antes de iniciar **ricci**, debe asegurarse de haber configurado su sistema así:

1. Los puertos IP en sus nodos de clúster deben habilitarse para **ricci**. Para obtener mayor información sobre cómo habilitar los puertos IP en nodos de clúster, consulte la Sección 2.3.1, “Cómo habilitar puertos IP en nodos de clúster”.
2. El servicio **ricci** se instala en todos los nodos en el clúster y asigna una contraseña **ricci**, como se describe en la Sección 2.13, “Consideraciones para **ricci**”.

Después de que **ricci** haya sido instalado y configurado en cada nodo, inicie el servicio de **ricci** en cada nodo:

```
# service ricci start
Starting ricci:                                            [  OK  ]
```

5.4. Cómo crear un clúster

Esta sección describe cómo crear, modificar y borrar un esqueleto de configuración de clúster con el comando **ccs** sin dominios de conmutación de cercado y servicios de alta disponibilidad. Las siguientes secciones describen cómo establecer esas partes de la configuración.

Para crear un esqueleto de archivo de configuración de clúster, primero cree un clúster y póngale un nombre, luego añada los nodos al clúster, como en el siguiente procedimiento:

1. Crear un archivo de configuración de clúster en uno de los nodos en el clúster al ejecutar el comando **ccs** mediante el parámetro **-h** para especificar el nodo en el cual crear el archivo y la opción **createcluster** para especificar un nombre para el clúster:

   ```
   ccs -h host --createcluster clustername
   ```

   Por ejemplo, el siguiente comando crea un archivo de configuración en **node-01.example.com** llamado **mycluster**:

   ```
   ccs -h node-01.example.com --createcluster mycluster
   ```

   usterEl nombre de clúster no puede exceder a 15 caracteres.

   Si un archivo **cluster.conf** ya existe en el host que usted especificó, ejecute este comando para remplazar el archivo existente.

   Si desea crear un archivo de configuración de clúster en su sistema local, puede especificar la opción **-f** en lugar de la opción **-h**. Para obtener mayor información sobre cómo crar el archivo de forma local, consulte la Sección 5.1.1, “Cómo crear un archivo de configuración de clúster en un sistema local”.
2. Para configurar los nodos que contiene el clúster, ejecute el siguiente comando para cada nodo en el clúster.

   ```
   ccs -h host --addnode nodo
   ```

   Por ejemplo, los siguientes tres comandos añaden los nodos **node-01.example.com**, **node-02.example.com**, y **node-03.example.com** al archivo de configuración en **node-01.example.com**:

   ```
   ccs -h node-01.example.com --addnode node-01.example.com
   ccs -h node-01.example.com --addnode node-02.example.com
   ccs -h node-01.example.com --addnode node-03.example.com
   ```

   Para ver una lista de los nodos que han sido configurados para un clúster, ejecute el siguiente comando:

   ```
   ccs -h host --lsnodes
   ```

   Ejemplo 5.1, “Archivo **cluster.conf** después de añadir tres nodos” muestra un archivo de configuración **cluster.conf** después de haber creado clúster **mycluster** que contiene los nodos **node-01.example.com**, **node-02.example.com**, y **node-03.example.com**.

Ejemplo 5.1. Archivo cluster.conf después de añadir tres nodos

```
<cluster name="mycluster" config_version="2">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Cuando usted añade un nodo al clúster, puede especificar el nombre de votos que el nodo aporta para determinar si hay cuórum. Para establecer el número de votos para un nodo de clúster, use el siguiente comando:

```
ccs -h host --addnode host --votes votos
```

Cuando usted añade un nodo, **ccs** asigna al nodo un número entero único que sirve de identificador de nodo. Si desea especificar el nodo de forma manual cuando cree un nodo, use el siguiente comando:

```
ccs -h host --addnode host --nodeid nodeid
```

Para retirar un nodo de un clúster, ejecute el siguiente comando:

```
ccs -h host --rmnode nodo
```

Cuando haya terminado todos los componentes de su clúster, necesitará sincronizar el archivo de configuración de clúster para todos los nodos, como se describe en la Sección 5.15, "Cómo propagar el archivo de configuración a los nodos de clúster".

5.5. Cómo configurar dispositivos de valla

La configuración de dispositivos de vallas consiste en crear, actualizar y borrar dispositivos de vallas para el clúster. Debe configurar los dispositivos de vallas en un clúster antes de configurar el cercado para los nodos en el clúster. Para obtener mayor información sobre cómo configurar vallas para los nodos individuales en el clúster, consulte la Sección 5.7, "Cómo configurar cercado para miembros de clúster".

Antes de configurar sus dispositivos de valla, debería modificar algunas de las propiedades de demonio de valla para su sistema de los valores predeterminados. Los valores que configure para el demonio del cercado son valores generales para el clúster. Las propiedades generales de cercado para el clúster que usted podría modificar se resumen a continuación:

- El atributo **post_fail_delay** es el número de segundos que el demonio de valla (**fenced**) espera antes de cercar un nodo (un miembro de un dominio de valla) después de que el nodo haya fallado. El valor predeterminado **post_fail_delay** es **0**. Su valor puede variar para ajustarse al rendimiento de clúster y red.
- El atributo **post-join_delay** es el número de segundos que el demonio de valla (**fenced**) espera antes de cercar un nodo después de que el nodo se enlace al dominio. El valor predeterminado de **post_join_delay** es **6**. El parámetro típico para **post_join_delay** está entre 20 y 30 segundos, pero puede variar según el rendimiento del clúster y de la red.

Restableció los valores de los atributos **post_fail_delay** y **post_join_delay** con la opción **--setfencedaemon** del comando **ccs**. Sin embargo, observe que la ejecución del comando **ccs --setfencedaemon** sobrescribe todas las propiedades del demonio de vallas existente que han sido establecidas y los restaura a sus valore predeterminados.

Por ejemplo, para configurar el valor para el atributo **post_fail_delay**, ejecute el siguiente comando. Este comando sobrescribirá los valores de las demás propiedades del demonio de valla existentes que usted haya establecido con este comando y los restaurará a sus valores predeterminados.

```
ccs -h host --setfencedaemon post_fail_delay=value
```

Para configurar el valor para el atributo **post_join_delay**, ejecute el siguiente comando. Este comando sobrescribirá los valores de las demás propiedades del demonio de valla existentes que usted haya establecido con este comando y los restaurará a sus valores predeterminados.

```
ccs -h host --setfencedaemon post_join_delay=value
```

Para configurar el valor para los atributos **post_join_delay** y **post_fail_delay**, ejecute el siguiente comando:

```
ccs -h host --setfencedaemon post_fail_delay=valor post_join_delay=valor
```

Nota

Para obtener mayor información sobre los atributos **post_join_delay** y **post_fail_delay** y de las propiedades del demonio de valla adicionales que usted puede modificar, consulte la página de manual fenced(8) y vaya al esquema de cluster en **/usr/share/cluster/cluster.rng**, y al esquema anotado en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Para configurar un dispositivo de valla para un clúster, ejecute el siguiente comando:

```
ccs -h host --addfencedev devicename [fencedeviceoptions]
```

Por ejemplo, para configurar un dispositivo de valla APC en el archivo de configuración en el nodo de clúster **node1** llamado **myfence** con una dirección IP de **apc_ip_example**, un nombre de inicio de **login_example**, y una contraseña de **password_example**, ejecute el siguiente comando:

```
ccs -h node1 --addfencedev myfence agent=fence_apc ipaddr=apc_ip_example
login=login_example passwd=password_example
```

El siguiente ejemplo muestra la sección **fencedevices** del archivo de configuración **cluster.conf** después de que le ha añadido este dispositivo de valla APC:

```
<fencedevices>
      <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="myfence" passwd="password_example"/>
</fencedevices>
```

Al configurar los dispositivos de valla para un clúster, puede ser útil ver un listado de los dispositivos disponibles para su clúster y las opciones para cada dispositivo. También puede hallar útil ver el listado de dispositivos de vallas actualmente configurados para su clúster. Para obtener información sobre el uso del comando **ccs** para imprimir una lista de dispositivos de vallas disponibles y opciones o para imprimir una lista de los dispositivos de vallas configurados actualmente, consulte la Sección 5.6, “Cómo listar dispositivos de vallas y opciones de dispositivos de vallas ”.

Para retirar un dispositivo de valla desde su configuración de clúster, ejecute el siguiente comando:

```
ccs -h host --rmfencedev fence_device_name
```

Por ejemplo, para retirar un dispositivo de valla que usted haya denominado **myfence** del archivo de configuración de clúster en un nodo de clúster **node1**, ejecute el siguiente comando:

```
ccs -h node1 --rmfencedev myfence
```

Si necesita modificar los atributos del dispositivo de valla que usted ya ha configurado, debe primero retirar ese dispositivo de valla y luego añadirlo de nuevo con los atributos modificados.

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

5.6. Cómo listar dispositivos de vallas y opciones de dispositivos de vallas

Puede utilizar el comando **ccs** para imprimir una lista de los dispositivos de vallas disponibles e imprimir una lista de opciones para cada tipo de valla disponible. También puede usar el comando **ccs** para imprimir una lista de los dispositivos de vallas actualmente configurados para su clúster.

Para imprimir una lista de los dispositivos disponibles actualmente para su clúster, ejecute el siguiente comando:

```
ccs -h host --lsfenceopts
```

Por ejemplo, el siguiente comando lista los dispositivos de vallas en el nodo de clúster **node1**, el cual muestra la salida de ejemplo.

```
[root@ask-03 ~]# ccs -h node1 --lsfenceopts
fence_rps10 - RPS10 Serial Switch
fence_vixel - No description available
fence_egenera - No description available
fence_xcat - No description available
fence_na - Node Assassin
fence_apc - Fence agent for APC over telnet/ssh
fence_apc_snmp - Fence agent for APC over SNMP
fence_bladecenter - Fence agent for IBM BladeCenter
fence_bladecenter_snmp - Fence agent for IBM BladeCenter over SNMP
fence_cisco_mds - Fence agent for Cisco MDS
fence_cisco_ucs - Fence agent for Cisco UCS
fence_drac5 - Fence agent for Dell DRAC CMC/5
fence_eps - Fence agent for ePowerSwitch
fence_ibmblade - Fence agent for IBM BladeCenter over SNMP
fence_ifmib - Fence agent for IF MIB
fence_ilo - Fence agent for HP iLO
fence_ilo_mp - Fence agent for HP iLO MP
fence_intelmodular - Fence agent for Intel Modular
fence_ipmilan - Fence agent for IPMI over LAN
fence_kdump - Fence agent for use with kdump
fence_rhevm - Fence agent for RHEV-M REST API
fence_rsa - Fence agent for IBM RSA
fence_sanbox2 - Fence agent for QLogic SANBox2 FC switches
fence_scsi - fence agent for SCSI-3 persistent reservations
fence_virsh - Fence agent for virsh
fence_virt - Fence agent for virtual machines
fence_vmware - Fence agent for VMware
fence_vmware_soap - Fence agent for VMware over SOAP API
fence_wti - Fence agent for WTI
fence_xvm - Fence agent for virtual machines
```

Para ver una lista de las opciones que puede especificar para un tipo específico de valla, ejecute el siguiente comando:

```
ccs -h host --lsfenceopts tipo_valla
```

Por ejemplo, el siguiente comando lista las opciones de comando para el agente **fence_wti**.

```
[root@ask-03 ~]# ccs -h node1 --lsfenceopts fence_wti
fence_wti - Fence agent for WTI
  Required Options:
  Optional Options:
    option: No description available
    action: Fencing Action
    ipaddr: IP Address or Hostname
    login: Login Name
    passwd: Login password or passphrase
    passwd_script: Script to retrieve password
    cmd_prompt: Force command prompt
    secure: SSH connection
    identity_file: Identity file for ssh
    port: Physical plug number or name of virtual machine
    inet4_only: Forces agent to use IPv4 addresses only
    inet6_only: Forces agent to use IPv6 addresses only
    ipport: TCP port to use for connection with device
    verbose: Verbose mode
    debug: Write debug information to given file
    version: Display version information and exit
    help: Display help and exit
    separator: Separator for CSV created by operation list
    power_timeout: Test X seconds for status change after ON/OFF
    shell_timeout: Wait X seconds for cmd prompt after issuing command
    login_timeout: Wait X seconds for cmd prompt after login
    power_wait: Wait X seconds after issuing ON/OFF
    delay: Wait X seconds before fencing is started
    retry_on: Count of attempts to retry power on
```

Para imprimir una lista de dispositivos de valla actualmente configurados para su clúster, ejecute

el siguiente comando:

```
ccs -h host --lsfencedev
```

5.7. Cómo configurar cercado para miembros de clúster

Cuando haya completado los pasos iniciales de creación de un clúster y dispositivos de valla, necesitará configurar el cercado para los nodos de clúster. Para configurar el cercado para los nodos tras crear un nuevo clúster y de configurar los dispositivo de valla para el clúster, siga los pasos en esta sección. Observe que debe configurar el cercado para cada nodo en el clúster.

Esta sección documenta los siguientes procedimientos:

- Sección 5.7.1, “Cómo configurar un dispositivo de valla basado en energía simple para un nodo”
- Sección 5.7.2, “Cómo configurar un dispositivo de valla basado en almacenamiento simple para un nodo”
- Sección 5.7.3, “Cómo configurar un dispositivo de valla de respaldo”
- Sección 5.7.4, “Cómo configurar un nodo con energía redundante”
- Sección 5.7.5, “Cómo retirar métodos de valla e instancias de valla ”

5.7.1. Cómo configurar un dispositivo de valla basado en energía simple para un nodo

Use el siguiente procedimiento para configurar un nodo con un dispositivo de valla de energía simple llamado **apc**, el cual usa el agente de cercado **fence_apc**.

1. Añada un método de valla para el nodo y proporciónele un nombre.

   ```
   ccs -h host --addmethod method node
   ```

   Por ejemplo, para configurar un método de valla denominado **APC** para el nodo **node-01.example.com** en el archivo de configuración en el nodo de cluster **node-01.example.com**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addmethod APC node01.example.com
   ```

2. Añada una instancia de cercado para el método. Especifique el dispositivo de valla a usar para el nodo, el nodo al que aplica esta instancia, el nombre del método y las opciones para este método que son específicas a este nodo.

   ```
   ccs -h host --addfenceinst nombredispositivoconmutación nodo método
   [opciones]
   ```

   Por ejemplo, para configurar una instancia de valla en el archivo de configuración en el nodo de cluster **node-01.example.com** que usa el puerto de alimentación 1 de interruptor APC en el dispositivo de valla llamado **apc** para nodo de cluster de valla **node-01.example.com** mediante el método denominado **APC**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addfenceinst apc node01.example.com APC port=1
   ```

Usted necesitará un método de valla para cada nodo en el cluster. Los siguientes comandos configuran un método de valla para cada nodo con el nombre del método **APC**. El dispositivo para el método de valla especifica **apc** como el nombre de dispositivo, el cual es un dispositivo que ha sido previamente configurado con la opción **--addfencedev**, como se describió en la Sección 5.5, “Cómo configurar dispositivos de valla”. Cada nodo es configurado con un número único de puerto de alimentación de interruptor APC: El número del puerto para **node-01.example.com** es **1**, el número de puerto para **node-02.example.com** es **2**, y el número de puerto para **node-03.example.com** es **3**.

```
ccs -h node01.example.com --addmethod APC node01.example.com
ccs -h node01.example.com --addmethod APC node02.example.com
ccs -h node01.example.com --addmethod APC node03.example.com
ccs -h node01.example.com --addfenceinst apc node01.example.com APC port=1
ccs -h node01.example.com --addfenceinst apc node02.example.com APC port=2
ccs -h node01.example.com --addfenceinst apc node03.example.com APC port=3
```

Ejemplo 5.2, “**cluster.conf** después de añadir métodos de valla basados en energía” muestra un archivo de configuración **cluster.conf** después de haber añadido estos métodos de cercado e instancias a cada nodo en el cluster.

Ejemplo 5.2. `cluster.conf` después de añadir métodos de valla basados en energía

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, "Cómo propagar el archivo de configuración a los nodos de clúster".

5.7.2. Cómo configurar un dispositivo de valla basado en almacenamiento simple para un nodo

Al utilizar métodos de valla sin-energía (es decir SAN/cercado de almacenamiento) para nodo de valla, debe configurar *unfencing* para el dispositivo de valla. Así asegura que el nodo cercado no sea reactivado hasta que el nodo haya reiniciado. Cuando configure el sin-cercado para un nodo, debe especificar un dispositivo que copie el dispositivo de valla correspondiente que ha configurado para el nodo con la adición notable de una acción explícita de **`on`** o **`enable`**.

Para obtener mayor información sobre cómo abrir un nodo, consulte a página de manual **`fence_node`**(8).

Use el siguiente procedimiento para configurar un nodo con un dispositivo de valla de almacenamiento simple que utiliza un dispositivo de valla denominado **`sanswitch1`**, el cual usa el agente de cercado **`fence_sanbox2`**.

1. Añada un método de valla para el nodo y proporciónele un nombre.

   ```
   ccs -h host --addmethod method node
   ```

   Por ejemplo, para configurar un método de valla denominado **`SAN`** para el nodo **`node-01.example.com`** en el archivo de configuración en el nodo de cluster **`node-01.example.com`**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addmethod SAN  node01.example.com
   ```

2. Añada una instancia de cercado para el método. Especifique el dispositivo de valla a usar para el nodo, el nodo al que aplica esta instancia, el nombre del método y las opciones para este método que son específicas a este nodo.

```
ccs -h host --addfenceinst nombredispositivoconmutación nodo método
[opciones]
```

Por ejemplo, para configurar una instancia de valla en el archivo de configuración en el nodo de cluster **node-01.example.com** que usa el puerto 11 de interruptor SAN en el dispositivo de valla llamado **sanswitch1** para nodo de cluster de valla **node-01.example.com** mediante el método llamado **SAN**, ejecute el siguiente comando:

```
ccs -h node01.example.com --addfenceinst sanswitch1 node01.example.com SAN
port=11
```

3. Para configurar la apertura para el dispositivo de vallas basado en almacenamiento en este nodo, ejecute el siguiente comando:

```
ccs -h host --addunfence nombredispositivoconmutación nodo action=on|off
```

Usted necesitará añadir un método de valla para cada nodo en el cluster. Los siguientes comandos configuran un método para cada nodo con el nombre del método **SAN**. El dispositivo para método de vallas especifica **sanswitch** como nombre de dispositivo, el cual es un dispositivo configurado anteriormente con la opción --addfencedev, como se describió en la Sección 5.5, "Cómo configurar dispositivos de valla". Cada nodo se configura con un número de puerto físico SAN único: El número de puerto para **node-01.example.com** es **11**, el número de puerto para **node-02.example.com** es **12**, y el número de puerto para **node-03.example.com** es **13**.

```
ccs -h node01.example.com --addmethod SAN node01.example.com
ccs -h node01.example.com --addmethod SAN node02.example.com
ccs -h node01.example.com --addmethod SAN node03.example.com
ccs -h node01.example.com --addfenceinst sanswitch1 node01.example.com SAN
port=11
ccs -h node01.example.com --addfenceinst sanswitch1 node02.example.com SAN
port=12
ccs -h node01.example.com --addfenceinst sanswitch1 node03.example.com SAN
port=13
ccs -h node01.example.com --addunfence sanswitch1 node01.example.com port=11
action=on
ccs -h node01.example.com --addunfence sanswitch1 node02.example.com port=12
action=on
ccs -h node01.example.com --addunfence sanswitch1 node03.example.com port=13
action=on
```

Ejemplo 5.3, "**cluster.conf** Después de adicionar métodos de valla basados en almacenamientos" muestra un archivo de configuración **cluster.conf** después de haber añadido métodos de cercado, instancias de cercado, para cada nodo en el cluster.

Ejemplo 5.3. `cluster.conf` Después de adicionar métodos de valla basados en almacenamientos

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="SAN">
              <device name="sanswitch1" port="11"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="11" action="on"/>
         </unfence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="SAN">
              <device name="sanswitch1" port="12"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="12" action="on"/>
         </unfence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="SAN">
              <device name="sanswitch1" port="13"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="13" action="on"/>
         </unfence>
     </clusternode>
   </clusternodes>
   <fencedevices>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

5.7.3. Cómo configurar un dispositivo de valla de respaldo

Debe definir varios métodos de cercado para un nodo. Si el cercado falla mediante el primer método, el sistema intentará cercar el nodo con el segundo método, seguido de los otros métodos adicionales que usted haya configurado. Para configurar un método de cercado de respaldo para un nodo, configure dos métodos para un nodo, configurando una instancia de valla para cada método.

Nota

El orden en el que el sistema utilizará los métodos de cercado que usted ha configurado, sigue el orden en el archivo de configuración de cluster. El primer método que configure con el comando **ccs** es el método de cercado primario y el segundo método que usted configure es el método de cercado de respaldo. Para cambiar el orden, debe retirar el método de cercado primario del archivo de configuración y luego añadirlo de nuevo.

Observe que en cualquier momento puede imprimir una lista de métodos de valla e instancias configuradas actualmente para un nodo si ejecuta el siguiente comando. Si no especifica un nodo, este comando listará los métodos de valla e instancias actualmente configurados para todos los nodos.

```
ccs -h host --lsfenceinst [node]
```

Siga el siguiente procedimiento para configurar un nodo con un método de valla primario que utiliza un dispositivo de valla llamado **apc**, el cual usa el agente de valla **fence_apc** y un dispositivo de cercado de respaldo con un dispositivo de valla llamado **sanswitch1**, el cual emplea el agente de cercado **fence_sanbox2**. Puesto que el dispositivo **sanswitch1** es un agente de cercado basado en almacenamiento, usted necesitará configurar la apertura de la valla para ese dispositivo.

1. Añada el método de valla primario para el nodo, proporcionando un nombre para el método de valla.

   ```
   ccs -h host --addmethod method node
   ```

   Por ejemplo, para configurar un método de valla llamado **APC** como el método primario para el nodo **node-01.example.com** en el archivo de configuración en el nodo de cluster **node-01.example.com**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addmethod APC node01.example.com
   ```

2. Añada una instancia de valla para método primario. Debe especificar el dispositivo de valla a usar para el nodo, el nodo al que esta instancia aplica, el nombre del método y cualquier otra opción para este método que sea específica a este nodo:

   ```
   ccs -h host --addfenceinst nombredispositivoconmutación nodo método
   [opciones]
   ```

   Por ejemplo, para configurar una instancia de valla en el archivo de configuración en el nodo de cluster **node-01.example.com** que usa el puerto de alimentación 1 de interruptor APC en el dispositivo de valla llamado **apc** para nodo de cluster de valla **node-01.example.com** mediante el método denominado **APC**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addfenceinst apc node01.example.com APC port=1
   ```

3. Añada un métod de valla de respaldo para el nodo, proporcionando un nombre para el método de valla.

   ```
   ccs -h host --addmethod method node
   ```

   Por ejemplo, para configurar un método de valla de respaldo llamado **SAN** para el nodo **node-01.example.com** en el archivo de configuración en el nodo de cluster **node-01.example.com**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addmethod SAN  node01.example.com
   ```

4. Añada una instancia de valla para el método de respaldo. Debe especificar el dispositivo de valla a usar para el nodo, el nodo al que se aplica esta instancia, el nombre del método y las opciones para este método que son específicas a este nodo:

   ```
   ccs -h host --addfenceinst nombredispositivoconmutación nodo método
   [opciones]
   ```

   Por ejemplo, para configurar una instancia de valla en el archivo de configuración en el nodo de cluster **node-01.example.com** que usa el puerto 11 de interruptor SAN en el dispositivo de valla llamado **sanswitch1** para nodo de cluster de valla **node-01.example.com** mediante el método llamado **SAN**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addfenceinst sanswitch1 node01.example.com SAN
   port=11
   ```

5. Puesto que el dispositivo **sanswitch1** es un dispositivo basado en almacenamiento, debe configurar el sin-cercado para este dispositivo.

   ```
   ccs -h node01.example.com --addunfence sanswitch1 node01.example.com
   port=11 action=on
   ```

Puede continuar añadiendo métodos de valla cuando se necesite.

Este procedimiento configura un dispositivo de valla y dispositivo de valla de respaldo para un nodo en el cluster. También necesitará configurar el cercado para los otros nodos en el cluster.

Ejemplo 5.4, “**cluster.conf** Después de añadir métodos de valla de respaldo” muestra un archivo de configuración **cluster.conf** tras haber añadido un método de respaldo primario

basado en energía y un método de cercado basado en almacenaje para cada nodo en el cluster.

Ejemplo 5.4. `cluster.conf` Después de añadir métodos de valla de respaldo

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
            <method name="SAN">
              <device name="sanswitch1" port="11"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="11" action="on"/>
         </unfence
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
            <method name="SAN">
              <device name="sanswitch1" port="12"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="12" action="on"/>
         </unfence
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
            <method name="SAN">
              <device name="sanswitch1" port="13"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="13" action="on"/>
         </unfence
     </clusternode>
   </clusternodes>
   <fencedevices>
        <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

Nota

El orden en el que el sistema utilizará los métodos de cercado que usted ha configurado, sigue el orden en el archivo de configuración de cluster. El primer método que configure es el método de cercado primario y el segundo método que usted configure es el método de cercado de respaldo. Para cambiar el orden, debe retirar el método de cercado primario del archivo de configuración y luego añadirlo de nuevo.

5.7.4. Cómo configurar un nodo con energía redundante

Si su cluster está configurado con fuentes de alimentación redundantes para sus nodos, debe asegurarse de configurar el cercado para que sus nodos se apaguen completamente cuando necesiten cercarse. Si configura cada fuente de alimentación como un método de valla independiente; la segunda fuente alimentadora permitirá al sistema continuar ejecutándose cuando la primera fuente de alimentación se cerque y el sistema no será cercado en absoluto. Para configurar un sistema con fuentes de alimentación duales, debe configurar los dispositivos de valla para que ambas fuentes de alimentación se apaguen y el sistema se considere completamente apagado. Se requiere que usted configure dos instancias dentro de un método de cercado único y que para cada instancia configure ambos dispositivos de valla con una atributo **action** de **off** antes de configurar cada uno de los dispositivos con un atributo de **action on**.

Para configurar el cercado para un nodo con abastecimiento de energía dual, siga los pasos a continuación en estas sección.

1. Antes de configurar el cercado para un nodo con energía redundante, debe configurar cada uno de los interrruptores como un dispositivo de valla para el cluster. Para obtener mayor información sobre cómo configurar dispositivos de valla, consulte la Sección 5.5, “Cómo configurar dispositivos de valla”.

   Para imprimir una lista de dispositivos de valla actualmente configurados para su clúster, ejecute el siguiente comando:

   ```
   ccs -h host --lsfencedev
   ```

2. Añada un método de valla para el nodo y proporciónele un nombre.

   ```
   ccs -h host --addmethod method node
   ```

   Por ejemplo, para configurar un método de valla llamado **APC-dual** para el nodo **node-01.example.com** en el archivo de configuración en el nodo de cluster **node-01.example.com**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addmethod APC-dual node01.example.com
   ```

3. Añada una instancia de valla para la primera fuente de alimentación a un método de valla. Debe especificar el dispositivo de valla a usar para el nodo, el nodo al que esta instancia se aplica, el nombre del método y las opciones para este método que son específicas a este nodo. En este mometo configure el atributo **action** como **off**.

   ```
   ccs -h host --addfenceinst fencedevicename node method [options]
   action=off
   ```

   Por ejemplo, para configurar una instancia de valla en el archivo de configuración en el nodo de cluster **node-01.example.com** que utiliza el puerto1 de interruptor APC denominado **apc1** para cercar el nodo de cluster **node-01.example.com** mediante el método denominado **APC-dual**, y establecer el atributo **action** a **off**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addfenceinst apc1 node01.example.com APC-dual
   port=1 action=off
   ```

4. Añada una instancia de valla para la segunda fuente de alimentación al método de valla. Debe especificar el dispositivo de valla a usar para el nodo, el nodo al que esta instancia se aplica, el nombre del método y las opciones para este método que sean específicas para este nodo. En este momento configure el atributo **action** como **off** para esta instancia también:

   ```
   ccs -h host --addfenceinst fencedevicename node method [options]
   action=off
   ```

Por ejemplo, para configurar una segunda instancia de valla en el archivo de configuración en el nodo de cluster **node-01.example.com** que utiliza el puerto1 de interruptor APC en el dispositivo de valla denominado **apc2** para nodo de cluster de valla **node-01.example.com** con el mismo método que usted especificó para la primera instancia denominado **APC-dual**, y configurando el atributo **action** a **off**, ejecute el siguiente comando:

```
ccs -h node01.example.com --addfenceinst apc2 node01.example.com APC-dual
port=1 action=off
```

5. Añada otra instancia para primera fuente de alimentación para el método de valla, configurando el atributo **action** como **on**. Debe especificar el dispositivo de valla a usar para el nodo, el nodo al que se aplica esta instancia, el nombre del método y las opciones para este método que son específicas para dicho nodo y especificando el atributo **action** como **on**:

   ```
   ccs -h host --addfenceinst fencedevicename node method [options] action=on
   ```

   Por ejemplo, para configurar una instancia de valla en el archivo de configuración en el nodo del clúster **node-01.example.com** que utiliza el puerto 1 del interruptor APC en el dispositivo de valla denominado **apc1** para cercar nodo de clúster **node-01.example.com** mediante el mismo método llamado **APC-dual**, y estableciendo el atributo **action** a **on**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addfenceinst apc1 node01.example.com APC-dual
   port=1 action=on
   ```

6. Añada otra instancia para segunda fuente de alimentación para el método de valla especificando el atributo **action** como **on** para esta instancia. Debe especificar el dispositivo de valla a usar para el nodo, el nodo a la que se aplica esta instancia, el nombre del método y las opciones para este método que son específicas para este nodo como también el atributo **action** de **on**.

   ```
   ccs -h host --addfenceinst fencedevicename node method [options] action=on
   ```

   Por ejemplo, para configurar una segunda instancia de valla en el archivo de configuración en el nodo de clúster **node-01.example.com** que utiliza el puerto 1 del interruptor APC en el dispositivo de valla denominado **apc2** para nodo de clúster de valla **node-01.example.com** con el mismo método que especificó para la primera instancia denominado **APC-dual** y configurando el atributo **action** a **on**, ejecute el siguiente comando:

   ```
   ccs -h node01.example.com --addfenceinst apc2 node01.example.com APC-dual
   port=1 action=on
   ```

Ejemplo 5.5, “**cluster.conf** Después de añadir cercado de energía dual” muestra un archivo de configuración **cluster.conf** después de haber añadido cercado para dos fuentes de alimentación a cada nodo en un clúster.

Ejemplo 5.5. `cluster.conf` Después de añadir cercado de energía dual

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="1"action="off"/>
              <device name="apc2" port="1"action="off"/>
              <device name="apc1" port="1"action="on"/>
              <device name="apc2" port="1"action="on"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="2"action="off"/>
              <device name="apc2" port="2"action="off"/>
              <device name="apc1" port="2"action="on"/>
              <device name="apc2" port="2"action="on"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="3"action="off"/>
              <device name="apc2" port="3"action="off"/>
              <device name="apc1" port="3"action="on"/>
              <device name="apc2" port="3"action="on"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
       <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc1" passwd="password_example"/>
       <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc2" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

5.7.5. Cómo retirar métodos de valla e instancias de valla

Para retirar un método de valla de su configuración de clúster, ejecute el siguiente comando:

```
ccs -h host --rmmethod método nodo
```

Por ejemplo, para retirar un método de valla que haya denominado **APC** y configurado para **node01.example.com** del archivo de configuración de clúster en el nodo de clúster **node01.example.com**, ejecute el siguiente comando:

```
ccs -h node01.example.com  --rmmethod APC node01.example.com
```

Para retirar todas las instancias de valla de un dispositivo de un método de valla, ejecute el siguiente comando:

```
ccs -h host --rmfenceinst nombredispositivodevalla nodo método
```

Por ejemplo, para retirar todas las instancias del dispositivo de valla denominado **apc1** del método llamado **APC-dual** configurado para **node01.example.com** desde el archivo de configuración en el nodo de clúster **node01.example.com**, ejecute el siguiente comando:

```
ccs -h node01.example.com --rmfenceinst apc1 node01.example.com APC-dual
```

5.8. Cómo configurar un dominio de conmutación

Un dominio de conmutación es un subconjunto de nodos de clúster elegible para ejecutar el servicio de clúster en el evento de una falla de nodo. Un dominio de conmutación puede tener las siguientes características:

- Sin restricciones — Le permite especificar que un subconjunto de miembros es preferido, pero que un servicio de clúster asignado a este dominio puede ejecutarse en cualquier miembro disponible.
- Restringido — Le permite restringir los miembros que pueden ejecutar un determinado servicio de clúster. Si ninguno de los miembros en un dominio de conmutación está disponible, el servicio de clúster no puede ser iniciado (ya sea manualmente o por el software de clúster).
- Desordenado — Cuando un servicio de clúster es asignado a un dominio de conmutación desordenado, el miembro en el cual el servicio de clúster se ejecuta es seleccionado de los miembros de dominio de conmutación disponibles sin ningún orden de prioridad.
- Ordenado — Le permite especificar un orden de preferencia entre los miembros de dominio de conmutación. El miembro en la parte superior de la lista es el preferido, seguido del segundo en la lista y así sucesivamente.
- Recuperación — Le permite especificar si un servicio en dominio de conmutación debe conmutar al nodo que originalmente se está ejecutando antes de que el nodo falle. La configuración de esta característica es útil en las circunstancias en las que un nodo repetidamente falla y es parte de un dominio de de recuperación ordenado. En esas circunstancias, si el nodo es el nodo preferido en un dominio de conmutación, es posible que un servicio se recupere y conmute repetidamente entre el nodo preferido y otro nodo, causando un grave impacto en el rendimiento.

Nota

La característica de conmutación se aplica solamente si la conmutación ordenada está configurada.

Nota

El cambio de una configuración de dominio de conmutación no se efectúa en servicios que están ejecutándose.

Nota

Los dominios de conmutación *no* se requieren para funcionar.

Por defecto, los dominios de conmutación no tienen orden ni restricciones.

En un clúster con varios miembros, mediante un dominio restringido de conmutación puede minimizar la labor de configuración del clúster para ejecutar un servicio de clúster (como **httpd**), el cual requiere que establezca de forma idéntica la configuración en todos los miembros que ejecutan el servicio de clúster. En lugar de configurar todo el clúster para que ejecute el servicio de clúster, puede configurar únicamente los miembros en un dominio de conmutación restringido que usted asocie con el servicio de clúster.

Nota

Para configurar un miembro preferido, puede crear un dominio de conmutación no restringido que comprenda únicamente un miembro de clúster. Al hacer esto, el servicio de clúster se ejecuta en ese miembro de clúster en primer lugar (el miembro preferido), pero permite al servicio de clúster conmutarse por recuperación a cualquiera de los otros miembros.

Para configurar un dominio de conmutación, realice lo siguiente:

1. Para añadir un dominio de conmutación, ejecute el siguiente comando:

   ```
   ccs -h host --addfailoverdomain nombre [restringido] [ordenado]
   [sinrecuperación]
   ```

   Nota

   El nombre debe ser lo suficientemente descriptivo para distinguir su propósito relativo a otros nombres usados en su clúster.

   Por ejemplo, el siguiente comando configura el dominio de conmutación denominado **example_pri** en **node-01.example.com** sin restricciones, ordenado y que permite la recuperación:

   ```
   ccs -h node-01.example.com --addfailoverdomain example_pri ordered
   ```

2. Para añadir un nodo a un dominio de conmutación, ejecute el siguiente comando:

   ```
   ccs -h host --addfailoverdomainnode dominiodeconmutación nodo prioridad
   ```

   Por ejemplo, para configurar el dominio de conmutación **example_pri** en el archivo de configuración en **node-01.example.com** para que contenga **node-01.example.com** con una prioridad de 1, **node-02.example.com** con una prioridad de 2, y **node-03.example.com** con una prioridad de 3, ejecute los siguientes comandos:

   ```
   ccs -h node-01.example.com --addfailoverdomainnode example_pri node-
   01.example.com 1
   ccs -h node-01.example.com --addfailoverdomainnode example_pri node-
   02.example.com 2
   ccs -h node-01.example.com --addfailoverdomainnode example_pri node-
   03.example.com 3
   ```

Puede listar los dominios de conmutación y los nodos de recuperación configurados en un cluster con el siguiente comando:

```
ccs -h host --lsfailoverdomain
```

Para retirar un dominio de conmutación, ejecute el siguiente comando:

```
ccs -h host --rmfailoverdomain nombre
```

Para retirar un nodo de un dominio de conmutación, ejecute el siguiente comando:

```
ccs -h host --rmfailoverdomainnode dominiodeconmutación nodo
```

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

5.9. Cómo configurar recursos de clúster global

Puede configurar dos tipos de recursos:

- Global — Recursos que están disponibles para cualquier servicio en el clúster.
- Específico-servicios — Recursos que están disponibles únicamente para un servicio.

Para ver una lista de los recursos y servicios configurados actualmente en el clúster, ejecute el siguiente comando:

```
ccs -h host --lsservices
```

Para añadir un recurso de clúster global, ejecute el siguiente comando. Puede añadir un recurso que sea local a un servicio determinado cuando configure el servicio, como se describe en la Sección 5.10, “Adición de un servicio de clúster al clúster”.

```
ccs -h host --addresource resourcetype [resource options]
```

Por ejemplo, el siguiente comando añade un recurso de sistema de archivos global al archivo de configuración de clúster en **node01.example.com**. El nombre del recurso es **web_fs**, el dispositivo de sistema de archivos es **/dev/sdd2**, el punto de montaje del sistema de archivos es **/var/www**, y el tipo de sistema de archivos es **ext3**.

```
ccs -h node01.example.com --addresource fs name=web_fs device=/dev/sdd2
mountpoint=/var/www fstype=ext3
```

Para obtener información sobre tipos de recursos y opciones de recursos disponibles, consulte el Apéndice B, *Parámetros de recursos de alta disponibilidad*.

Para retirar un recurso global, ejecute el siguiente comando:

```
ccs -h host --rmresource tipoderecurso [opciones de recursos]
```

Si necesita modificar los parámetros de un recurso global existente, puede retirar el recurso y reconfigurarlo.

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, "Cómo propagar el archivo de configuración a los nodos de clúster".

5.10. Adición de un servicio de clúster al clúster

Para configurar un servicio de clúster en un clúster, realice los siguientes pasos:

1. Añadir un servicio del clúster con el siguiente comando:

   ```
   ccs -h host --addservice servicename [service options]
   ```

   

   Nota

   Use un nombre descriptivo que distinga claramente el servicio de otros servicios en el clúster.

   Al añadir un servicio a la configuración de un clúster, puede configurar los siguientes atributos:

   - **autostart** — Especifica si debe autoiniciar el servicio o no, cuando el clúster inicia. Use "1" para habilitar y "0" para inhabilitar; el predeterminado es habilitado.
   - **domain** — Especifica un dominio de conmutación (si se requiere).
   - **exclusive** — Especifica una política en la que el servicio solamente se ejecuta en nodos que no tienen otros servicios ejecutándose en ellos.
   - **recovery** — Especifica una política de recuperación para el servicio. Las opciones son reubicar, reiniciar, inhabilitar, o reiniciar-inhabilitar el servicio. La política de recuperación indica que el sistema debe intentar reiniciar el servicio fallido antes de tratar de reubicar el servicio a otro nodo. La política de reubicación indica que el sistema debe intentar reiniciar el servicio en un nodo diferente. La política indica que el sistema debe inhabilitar el grupo de recursos si algún componente falla. La política reiniciar-inhabilitar indica que el servicio debe intentar reiniciar el servicio en su lugar si falla, pero si al reiniciar el servicio falla, el servicio se inhabilitará en lugar de ser desplazado a otro host en el clúster.

     Si selecciona **Reiniciar** o **Reiniciar-Inhabilitar**como política de recuperación para el servicio, puede especificar el número máximo de fallas de reinicio antes de reubicar o desactivar el servicio y el tiempo en segundos después del cual olvida reiniciar.

   Por ejemplo, para añadir al archivo de configuración en un nodo de cluster **node-01.example.com** denominado **example_apache** que utiliza el dominio de conmutación por error **example_pri**, y tiene una directiva de recuperación de **relocate**, ejecute el siguiente comando:

   ```
   ccs -h node-01.example.com --addservice example_apache domain=example_pri
   recovery=relocate
   ```

   Al configurar servicios para un clúster, puede hallar útil ver un listado de servicios disponibles para su clúster y las opciones disponibles para cada servicio. Para obtener mayor información sobre cómo usar el comando **ccs** para imprimir una lista de los servicios y opciones disponibles, consulte la Sección 5.11, "Listado de cluster disponibles ".
2. Añadir recursos al servicio con el siguiente comando:

```
ccs -h host --addsubservice servicename subservice [service options]
```

Según el tipo de recursos que usted desee utilizar, rellene el servicio con recursos globales o específicos del servicio. Para añadir un recurso global, use la opción **--addsubservice** de **ccs** para añadir un recurso. Por ejemplo, para añadir un recurso de sistema de archivos global llamado **web_fs** al servicio llamado **example_apache** en el archivo de configuración de cluster **node-01.example.com**, ejecute el siguiente comando:

```
ccs -h node01.example.com --addsubservice example_apache fs ref=web_fs
```

Para añadir un recurso específico del servicio para el servicio, necesita especificar todas las opciones del servicio. Por ejemplo, si no lo ha definido previamente **web_fs** como un servicio global, podría añadirlo como un recurso específico del servicio con el siguiente comando:

```
ccs -h node01.example.com --addsubservice example_apache fs name=web_fs
device=/dev/sdd2 mountpoint=/var/www fstype=ext3
```

3. Para añadir un servicio hijo al servicio, debe usar la opción **--addsubservice** del comando **ccs**, especificando las opciones de servicio.

   Si necesita añadir servicios dentro de una estructura de árbol de dependencias, use dos puntos (":") para separar elementos y paréntesis para identificar subservicios del mismo tipo. El siguiente ejemplo añade un tercer servicio **nfsclient** de un servicio **nfsclient** es en sí mismo un subservicio de un servicio **nfsclient** el cual es un subservicio de un servicio llamado **service_a**:

   ```
   ccs -h node01.example.com --addsubservice service_a nfsclient[1]:nfsclient
   [2]:nfsclient
   ```

   Nota

   Si está añadiendo un recurso de servicio de Samba, añádalo directamente al servicio, *no* como un hijo de otro recurso.

Nota

Para verificar la existencia del recurso de servicios IP utilizado en un servicio de clúster, utilice el comando **/sbin/ip addr show** en un nodo de clúster (en lugar del comando obsoleto **ifconfig**). La siguiente salida muestra el comando **/sbin/ip addr show** ejecutado en un nodo que ejecuta un servicio de clúster:

```
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1356 qdisc pfifo_fast qlen 1000
    link/ether 00:05:5d:9a:d8:91 brd ff:ff:ff:ff:ff:ff
    inet 10.11.4.31/22 brd 10.11.7.255 scope global eth0
    inet6 fe80::205:5dff:fe9a:d891/64 scope link
    inet 10.11.4.240/22 scope global secondary eth0
       valid_lft forever preferred_lft forever
```

Para retirar un servicio en todos los subservicios, ejecute el siguiente comando:

```
ccs -h host --rmservice servicename
```

Para retirar un subservicio, ejecuta el siguiente comando:

```
ccs -h host --rmsubservice servicename subservice [service options]
```

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

5.11. Listado de cluster disponibles

Puede usar el comando **ccs** para imprimir una lista de servicios que están disponibles para un cluster. Puede también usar el comando **ccs** para imprimir una lista de las opciones que puede especificar para un servicio específico.

Para imprimir una lista de los servicios de cluster para su cluster, ejecute el siguiente comando:

```
ccs -h host --lsserviceopts
```

Por ejemplo, el siguiente comando lista los servicios de cluster disponibles en el nodo de cluster **node1**, que muestra la salida de ejemplo.

```
[root@ask-03 ~]# ccs -h node1 --lsserviceopts
service - Defines a service (resource group).
ASEHAagent - Sybase ASE Failover Instance
SAPDatabase - SAP database resource agent
SAPInstance - SAP instance resource agent
apache - Defines an Apache web server
clusterfs - Defines a cluster file system mount.
fs - Defines a file system mount.
ip - This is an IP address.
lvm - LVM Failover script
mysql - Defines a MySQL database server
named - Defines an instance of named server
netfs - Defines an NFS/CIFS file system mount.
nfsclient - Defines an NFS client.
nfsexport - This defines an NFS export.
nfsserver - This defines an NFS server resource.
openldap - Defines an Open LDAP server
oracledb - Oracle 10g Failover Instance
orainstance - Oracle 10g Failover Instance
oralistener - Oracle 10g Listener Instance
postgres-8 - Defines a PostgreSQL server
samba - Dynamic smbd/nmbd resource agent
script - LSB-compliant init script as a clustered resource.
tomcat-6 - Defines a Tomcat server
vm - Defines a Virtual Machine
action - Overrides resource action timings for a resource instance.
```

Para ver una lista de las opciones que puede especificar para un tipo de servicio específico, ejecute el siguiente comando:

```
ccs -h host --lsserviceopts tipo_servicio
```

Por ejemplo, el siguiente comando lista las opciones de servicio para el servicio **vm**.

```
[root@ask-03 ~]# ccs -f node1 --lsserviceopts vm
vm - Defines a Virtual Machine
  Required Options:
    name: Name
  Optional Options:
    domain: Cluster failover Domain
    autostart: Automatic start after quorum formation
    exclusive: Exclusive resource group
    recovery: Failure recovery policy
    migration_mapping: memberhost:targethost,memberhost:targethost ..
    use_virsh: If set to 1, vm.sh will use the virsh command to manage virtual
machines instead of xm. This is required when using non-Xen virtual machines
(e.g. qemu / KVM).
    xmlfile: Full path to libvirt XML file describing the domain.
    migrate: Migration type (live or pause, default = live).
    path: Path to virtual machine configuration files.
    snapshot: Path to the snapshot directory where the virtual machine image
will be stored.
    depend: Top-level service this depends on, in service:name format.
    depend_mode: Service dependency mode (soft or hard).
    max_restarts: Maximum restarts for this service.
    restart_expire_time: Restart expiration time; amount of time before a
restart is forgotten.
    status_program: Additional status check program
    hypervisor: Hypervisor
    hypervisor_uri: Hypervisor URI (normally automatic).
    migration_uri: Migration URI (normally automatic).
    __independent_subtree: Treat this and all children as an independent
subtree.
    __enforce_timeouts: Consider a timeout for operations as fatal.
    __max_failures: Maximum number of failures before returning a failure to a
status check.
    __failure_expire_time: Amount of time before a failure is forgotten.
    __max_restarts: Maximum number restarts for an independent subtree before
giving up.
    __restart_expire_time: Amount of time before a failure is forgotten for an
independent subtree.
```

5.12. Recursos de máquinas virtuales

Los recursos de máquina virtual se configuran de una forma diferente a la de los recursos de clúster. En particular, no se agrupan en definiciones de servicios. A partir del lanzamiento de Red Hat Enterprise Linux 6.2, cuando configure una máquina virtual en un clúster con el comando **ccs**, puede usar la opción **--addvm** (en lugar de la opción **addservice**). Así garantiza que el recurso de **vm** se defina directamente bajo el nodo de configuración **rm** en el archivo de configuración de clúster.

Un recurso de máquina virtual requiere por lo menos un atributo **name** y un atributo **path**. El atributo **name** debe coincidir con el nombre del dominio **libvirt** y el atributo **path** debe especificar el directorio donde se almacenan las definiciones de máquina virtual compartidas .

Nota

El atributo **path** en el archivo de configuración de clúster es una especificación de ruta o nombre de directorio, no una ruta a un archivo individual.

Si las definiciones de máquina virtual se almacenan y comparten en un directorio compartido denominado **/mnt/vm_defs**, el siguiente comando definirá una máquina virtual denominada **guest1**:

```
# ccs -h node1.example.com --addvm guest1 path=/mnt/vm_defs
```

Al ejecutar este comando añada la siguiente línea al nodo de configuración **rm** en el archivo **cluster.conf**:

```
<vm name="guest1" path="/mnt/vm_defs"/>
```

5.13. Cómo configurar un disco de cuórum

Importante

Los parámetros de disco de cuórum y heurística dependen del entorno del sitio y de los requisitos especiales que se necesiten. Para entender el uso de parámetros de disco de cuórum y heurística, consulte la página de manual qdisk(5). Si requiere asistencia para entender y utilizar disco de cuórum, contacte a un representante autorizado de soporte técnico de Red Hat.

Utilice el siguiente comando para configurar su sistema para que use un disco de cuórum:

```
ccs -h host --setquorumd [quorumd options]
```

Observe que este comando restablece las demás propiedades que usted puede establecer con la opción **--setquorumd** a sus valores predeterminados, así como se describe en la Sección 5.1.5, "Comandos que sobrescriben los parámetros anteriores".

Tabla 5.1, "Opciones de disco de cuórum" resume el significado de opciones de disco de cuórum que puede necesitar para la configuración. Para completar la lista de parámetros de disco de cuórum, consulte el esquema de cluster en **/usr/share/cluster/cluster.rng**, y el esquema anotado en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Tabla 5.1. Opciones de disco de cuórum

Parámetro	Descripción
intervalo	La frecuencia de ciclos de lectura/escritura, en segundos.
votos	El número de votos de demonio de cuórum se anuncia a **cman** cuando tiene un puntaje suficientemente alto.
tko	El número de ciclos que un nodo debe perder para ser declarado muerto.
puntaje_mín	El puntaje mínimo para considerar 'vivo' a un nodo. Si se omite o establece a 0, la función predeterminada, **floor((*n*+1)/2)**, se utiliza, donde ***n*** es la suma de puntajes de heurística. El valor de **Puntaje mínimo** nunca debe exceder la suma de los puntajes heurísticos; de lo contrario, el disco de cuórum no puede estar disponible.
dispositivo	El dispositivo de almacenamiento que el demonio de cuórum utiliza. El dispositivo debe ser el mismo en todos los nodos.
etiqueta	Especifica la etiqueta de disco de cuórum creado por la herramienta **mkqdisk**. Si este campo contiene una entrada, la etiqueta sobrescribe el campo de **Dispositivo**. Si el campo es utilizado, el demonio de cuórum lee **/proc/partitions** y chequea las firmas de qdisk en cada bloque de dispositivo encontrado, comparando las etiquetas con la etiqueta especificada. Esto es muy útil en configuraciones en las que el nombre de dispositivo de cuórum difiere entre nodos.

Use el siguiente comando para configurar la heurística para un disco de cuórum:

```
ccs -h host --addheuristic [heuristic options]
```

Tabla 5.2, "Heurística de disco de cuórum" resume el significado de la heurística de disco de cuórum necesaria.

Tabla 5.2. Heurística de disco de cuórum

Parámetro	Descripción
programa	La ruta al programa utilizado para determinar si esta heurística está disponible. Puede ser cualquiera que pueda ser ejecutada por **/bin/sh -c**. Un valor de retorno de 0 indica éxito; cualquier otro indica falla. Este parámetro es obligatorio para usar un disco de cuórum.
intervalo	La frecuencia (en segundos) en la cual se sondea la heurística. El intervalo predeterminado para cada heurística es de 2 segundos.
puntaje	El peso de esta heurística. Tenga cuidado al determinar el puntaje para heurística. El puntaje predeterminado para cada heurística es de 1.
tko	El número de fallas consecutivas antes de que esta heurística sea declarada no disponible.

Para ver una lista de opciones de disco de cuórum y heurística configurados en un sistema, ejecute el siguiente comando:

```
ccs -h host --lsquorum
```

Para retirar una heurística especificada por una opción de heurística, ejecute el siguiente comando:

```
ccs -h host rmheuristic [opciones de heurística]
```

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

Nota

Al sincronizar y activar propaga y activa el archivo de configuración de clúster. No obstante, para que el disco de cuórum funcione, debe reiniciar el clúster (consulte la Sección 6.2, “Cómo iniciar y detener un clúster”), para asegurarse de que haya reiniciado el demonio **qdiskd** en cada nodo.

5.14. Varios de configuración de clúster

Esta sección describe el uso del comando **ccs** para configurar lo siguiente:

- Sección 5.14.1, “Versión de configuración de clúster”
- Sección 5.14.2, “Configuración de multidifusión”
- Sección 5.14.3, “Cómo configurar un clúster de dos nodos”
- Sección 5.14.4, “Registro”
- Sección 5.14.5, “Cómo configurar el protocolo de anillo redundante”

También puede usar el comando **ccs** para establecer los parámetros de configuración de clúster avanzados, incluyendo las opciones de **totem**, **dlm**, **rm** y **cman**. Para obtener información sobre configuración de estos parámetros, consulte la página de manual **ccs**(8) y el esquema de archivo de configuración de clúster en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Para ver una lista de los varios atributos de clúster que han sido configurados para un clúster, ejecute el siguiente comando:

```
ccs -h host --lsmisc
```

5.14.1. Versión de configuración de clúster

Un archivo de configuración de clúster incluye un valor de versión de configuración de clúster. El valor de versión de configuración se predetermina a **1** cuando usted crea un archivo de configuración de clúster. Sin embargo, si necesita establecerlo a otro valor, puede especificarlo con el siguiente comando:

```
ccs -h host --setversion n
```

Puede obtener el valor de versión de configuración actual en un archivo de configuración de clúster existente con el siguiente comando:

```
ccs -h host --getversion
```

Para incrementar el valor de versión actual en 1 en el archivo de configuración en cada nodo en el clúster, ejecute el siguiente comando:

```
ccs -h host --incversion
```

5.14.2. Configuración de multidifusión

Si no especifica una dirección de multidifusión en el archivo de configuración de clúster, el software de adición de alta disponibilidad de Red Hat crea uno basado en el ID de clúster. Dicho ID genera los 16 bits inferiores de la dirección y los añade a la porción superior de la dirección según el protocolo IP ya sea IPV4 o IPV6:

- Para IPV4 — La dirección formada es 239.192. más los 16 bits inferiores generados por el software de adición de alta disponibilidad de Red Hat.
- Para IPV6 — La dirección formada es FF15:: más la inferior de 16 bits generada por software de adición de alta disponibilidad de Red Hat.

Nota

El ID de clúster es un identificador único que **cman** genera para cada clúster. Para ver el ID de clúster, ejecute el comando **cman_tool status** en un nodo de clúster.

Puede especificar manualmente una dirección de multidifusión en el archivo de configuración de clúster con el siguiente comando:

```
ccs -h host --setmulticast direcciónmultidifusión
```

Observe que este comando restablece las demás propiedades que usted puede establecer con la opción **--setmulticast** a sus valores predeterminados, así como se describe en la Sección 5.1.5, “Comandos que sobrescriben los parámetros anteriores”.

Si especifica una dirección de multidifusión, debe usar las series 239.192.x.x (o FF15:: para IPv6) que utiliza **cman**. De lo contrario, el uso de una dirección de multidifusión fuera de ese rango puede causar resultados impredecibles. Por ejemplo, el uso de 224.0.0.x (la cual es "Todos los hosts en la red") puede que no se pueda dirigir correctamente, o incluso que no se pueda dirigir en absoluto por ningún hardware.

Si especifica o modifica una dirección multidifusión, debe reiniciar el clúster para que se efectúe. Para mayor información sobre iniciar y detener un clúster con el comando **ccs**, consulte la Sección 6.2, “Cómo iniciar y detener un clúster”.

Nota

Si especifica una dirección de multidifusión, asegúrese de revisar la configuración de enrutadores por los que pasan los paquetes. Algunos enrutadores pueden tardar en aprender direcciones, impactando seriamente el rendimiento del clúster.

Para retirar una dirección de multidifusión del archivo de configuración, use la opción **--setmulticast** de **ccs** pero no especifique una dirección de multidifusión:

```
ccs -h host --setmulticast
```

5.14.3. Cómo configurar un clúster de dos nodos

Si está configurando un clúster de dos nodos, puede ejecutar el siguiente comando para permitir que un nodo simple mantenga cuórum (por ejemplo, si un nodo falla):

```
ccs -h host --setcman two_node=1 expected_votes=1
```

Observe que este comando restablece las demás propiedades que usted puede establecer con la opción **--setcman** a sus valores predeterminados, así como se describe en la Sección 5.1.5, "Comandos que sobrescriben los parámetros anteriores".

Cuando use el comando **ccs --setcman** para añadir, retirar o modificar la opción **two_node**, debe reiniciar el cluster para que este cambio se efectúe. Para obtener información sobre cómo iniciar o detener un clúster con el comando **ccs** consulte, Sección 6.2, "Cómo iniciar y detener un clúster".

5.14.4. Registro

Puede activar la depuración para todos los demonios en un clúster o puede habilitar el registro para procesamiento de clúster específico.

Para activar la depuración en todos los demonios, ejecute el siguiente comando. Por defecto, el registro se dirige al archivo **/var/log/cluster/*daemon*.log**.

```
ccs -h host --setlogging [opciones de registro]
```

Por ejemplo, el siguiente comando activa la depuración para todos los demonios.

```
# ccs -h node1.example.com --setlogging debug=on
```

Observe que este comando restablece las demás propiedades que usted puede establecer con la opción **--setlogging** a sus valores predeterminados, así como se describe en la Sección 5.1.5, "Comandos que sobrescriben los parámetros anteriores".

Para activar la depuración para un proceso de clúster individual, ejecute el siguiente comando. La configuración del registro por demonio sobrescribe los parámetros globales.

```
ccs -h host --addlogging [logging daemon options]
```

Por ejemplo, los siguientes comandos activan la depuración para los demonios **corosync** y **fenced**.

```
# ccs -h node1.example.com --addlogging name=corosync debug=on
# ccs -h node1.example.com --addlogging name=fenced debug=on
```

Para retirar los parámetros de registro para los demonios individuales, use el siguiente comando.

```
ccs -h host --rmlogging name=clusterprocess
```

Por ejemplo, el siguiente comando retira los parámetros de registro del demonio específico para el demonio **fenced**.

```
ccs -h host --rmlogging name=fenced
```

Para obtener un listado de los demonios de registro, con los cuales puede habilitar el registro así como las opciones de registro adicionales que se pueden configurar para el registro global y para el registro por demonio, consulte la página de manual **cluster.conf**(5).

Observe que cuando hay terminado de configurar todos los componentes de su clúster, necesitará sincronizar el archivo de configuración para todos los nodos, como se describe en la Sección 5.15, "Cómo propagar el archivo de configuración a los nodos de clúster".

5.14.5. Cómo configurar el protocolo de anillo redundante

A partir de Red Hat Enterprise Linux 6.4, la adición de alta disponibilidad de Red Hat soporta la configuración del protocolo de anillos redundantes. Cuando utilice el protocolo de anillos redundantes, se debe tener en cuenta un gran número de consideraciones como se describe en la Sección 7.6, "Cómo configura el protocolo de anillos redundantes".

Para especificar una segunda interfaz de red para usar protocolo de anillos redundantes, añada un nombre alternativo mediante la opción **--addalt** del comando **ccs**:

```
ccs -h host --addalt nombre_nodo nombre_alt
```

Por ejemplo, el siguiente comando configura el nombre alternativo **clusternet-node1-eth2** para el nodo de clúster **clusternet-node1-eth1**:

```
# ccs -h clusternet-node1-eth1 --addalt clusternet-node1-eth1 clusternet-node1-
eth2
```

También, puede especificar de forma manual una dirección multidifusión para el segundo anillo. Si especifica multidifusión para el segundo anillo, ya sea la dirección multidifusión alterna o el puerto alterno debe ser diferente a la dirección multidifusión para el primer anillo. Si especifica un puerto alterno, los números de puerto del primer anillo y el segundo anillo deben diferir en al menos 2, puesto que el sistema mismo usa 'Port' y 'Port -1' para realizar operaciones. Si no desea especificar una dirección multidifusión, el sistema usará automáticamente la dirección multidifusión para el segundo anillo.

Para especificar una dirección multidifusión, puerto o TTL para el segundo anillo, utilice la opción **--setaltmulticast** del comando **ccs**:

```
ccs -h host --setaltmulticast [dirección_multidifusión_alt]
[opciones_multidifusión_alt].
```

Por ejemplo, el siguiente comando establece una dirección multidifusión alterna de 239.192.99.88, un puerto de 888, y un TTL de 3 para el clúster definido en el archivo **cluster.conf** en nodo **clusternet-node1-eth1**:

```
ccs -h clusternet-node1-eth1 --setaltmulticast 239.192.99.88 port=888 ttl=3
```

Para retirar una dirección multidifusión alterna, especifique la opción **--setaltmulticast** del comando **ccs** pero no especifique una dirección multidifusión. Observe que al ejecutar este comando restablece las demás propiedades que usted puede establecer a sus valores predeterminados con la opción **--setaltmulticast**, así como se describe en la Sección 5.1.5, “Comandos que sobrescriben los parámetros anteriores”.

Cuando haya terminado todos los componentes de su clúster, necesitará sincronizar el archivo de configuración de clúster para todos los nodos, como se describe en la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

5.15. Cómo propagar el archivo de configuración a los nodos de clúster

Después de haber creado o editado un archivo de configuración de clúster en uno de los nodos en el clúster, necesita propagar ese mismo archivo a todos los nodos de clúster y activar la configuración.

Use el siguiente comando para propagar un archivo de configuración de clúster activo:

```
ccs -h host --sync --activate
```

Para verificar si todos los nodos especificados en el archivo de configuración de clúster de hosts tienen el archivo de configuración de clúster idéntico, ejecute el siguiente comando:

```
ccs -h host --checkconf
```

Si ha creado o editado un archivo de configuración en un nodo local, use el siguiente comando para enviar ese archivo a uno de los nodos en el clúster:

```
ccs -f archivo -h host --setconf
```

Para verificar si todos los nodos especificados en el archivo local tienen el archivo de configuración de clúster idéntico, ejecute el siguiente comando:

```
ccs -f file --checkconf
```

Capítulo 6. Administración de adición de alta disponibilidad de Red Hat con ccs

6.1. Administrar nodos de clúster
6.1.1. Hacer que un nodo abandone o se una a un clúster
6.1.2. Añadir un miembro a un clúster en ejecución
6.2. Cómo iniciar y detener un clúster
6.3. Cómo diagnosticar y corregir problemas en un clúster

Este capítulo describe varias tareas administrativas para el manejo de adición de alta disponibilidad de Red Hat por medio del comando **ccs**, el cual está soportado a partir del lanzamiento de Red Hat Enterprise Linux 6.1 y posterior. Este capítulo consta de las siguientes secciones:

- Sección 6.1, “Administrar nodos de clúster”
- Sección 6.2, “Cómo iniciar y detener un clúster”
- Sección 6.3, “Cómo diagnosticar y corregir problemas en un clúster”

6.1. Administrar nodos de clúster

Esta sección describe cómo realizar las siguientes funciones administrativas de nodos con el comando **ccs**:

- Sección 6.1.1, “Hacer que un nodo abandone o se una a un clúster”
- Sección 6.1.2, “Añadir un miembro a un clúster en ejecución”

6.1.1. Hacer que un nodo abandone o se una a un clúster

Puede usar el comando **ccs** para hacer que el nodo abandone el clúster deteniendo los servicios de clúster en ese nodo. Para que un nodo abandone un clúster no se necesita retirar del nodo la información de configuración de clúster. Al hacer que el nodo abandone el clúster evitará que el nodo se conecte automáticamente al clúster en el rearranque.

Para que el nodo abandone el clúster, ejecute el siguiente comando, el cual detiene los servicios de clúster en el nodo especificado con la opción **-h**:

```
ccs -h host --stop
```

Al detener los servicios de clúster en un nodo, cualquier servicio que esté ejecutándose en ese nodo fallará.

Para borrar un nodo completamente de la configuración de clúster, use la opción **--rmnode** del comando **ccs**, como se describión en Sección 5.4, “Cómo crear un clúster”.

Para hacer que un nodo se reconecte a un clúster ejecute el siguiente comando, el cual inicia servicios de clúster en el nodo especificado con la opción **-h**:

```
ccs -h host --start
```

6.1.2. Añadir un miembro a un clúster en ejecución

Para añadir un miembro de clúster en ejecución, añada un nodo al clúster como se describe en la Sección 5.4, “Cómo crear un clúster”. Tras actualizar el archivo de configuración, propague el archivo a todos los nodos en el clúster y asegúrese de activar el nuevo archivo de configuración de clúster, como se describe en Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.

6.2. Cómo iniciar y detener un clúster

Puede usar el comando **ccs** para detener un clúster con el siguiente comando para detener los servicios de clúster en todos los nodos en el clúster:

```
ccs -h host --stopall
```

Puede usar **ccs** para iniciar un clúster que no está ejecutándose mediante el siguiente comando para iniciar servicios de clúster en todos los nodos en el clúster:

```
ccs -h host --startall
```

6.3. Cómo diagnosticar y corregir problemas en un clúster

Para obtener información sobre cómo diagnosticar y corregir problemas en un clúster, consulte Capítulo 9, *Cómo diagnosticar y corregir problemas en un clúster*. No obstabte, hay algunas revisiones sencillas que usted puede realizar con el comando **ccs**.

Para verificar que todos los nodos especificados en el archivo de configuración de clúster del host tengan archivos de configuración idénticos, ejecute el siguiente comando:

```
ccs -h host --checkconf
```

Si ha creado o editado un archivo de configuración en un nodo local, puede verificar si todos los nodos especificados en el archivo local tienen archivos de configuración de clúster idénticos con el comando:

```
ccs -f file --checkconf
```

Capítulo 7. Configuración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos

7.1. Tareas de configuración

7.2. Creación de un archivo de configuración de clúster básico

7.3. Configuración de vallas

7.4. Configuración de dominios de conmutación

7.5. Configuración de servicios de alta disponibilidad
- 7.5.1. Adición de recursos de clúster
- 7.5.2. Adición de un servicio de clúster al clúster

7.6. Cómo configura el protocolo de anillos redundantes

7.7. Configuración de opciones de depuración

7.8. Verificación de una configuración

Este capítulo describe cómo configurar software de adición de alta disponibilidad de Red Hat al editar directamente el archivo de configuración de clúster (**/etc/cluster/cluster.conf**) y usar las herramientas de la línea de comandos. El capítulo proporciona procedimientos sobre la creación de una sola sección de archivo de configuración a la vez, iniciando por un archivo de muestra provisto en el capítulo. Como alternativa para iniciar con el archivo de muestra provisto aquí, puede copiar un archivo de configuración de esqueleto de la página de manual **cluster.conf**. No obstante, al hacerlo no se alinearía necesariamente con información provista en los procedimientos subsiguientes a este capítulo. Hay otras formas de crear y configurar un archivo de configuración de clúster: este capítulo provee procedimientos para la creación de un archivo de configuración de una sección a la vez. Tenga en cuenta que se trata solo del inicio para desarrollar un archivo de configuración que se ajuste a sus necesidades de agrupamiento.

Este capítulo consta de las siguientes secciones:

- Sección 7.1, “Tareas de configuración”
- Sección 7.2, “Creación de un archivo de configuración de clúster básico”
- Sección 7.3, “Configuración de vallas”
- Sección 7.4, “Configuración de dominios de conmutación”
- Sección 7.5, “Configuración de servicios de alta disponibilidad”
- Sección 7.7, “Configuración de opciones de depuración”
- Sección 7.6, “Cómo configura el protocolo de anillos redundantes”
- Sección 7.8, “Verificación de una configuración”

Importante

Asegúrese de que su adición de alta disponibilidad cumpla con sus necesidades y tenga soporte. Consulte a un representante autorizado de Red Hat para verificar su configuración antes de ejecutarla. Además, deje un tiempo de periodo de prueba para ensayar los modos de falla.

Importante

Este capítulo hace referencia a los elementos y atributos de **cluster.conf** más utilizados. Para obtener una lista y descripción completa de **cluster.conf**, consulte el esquema de cluster en **/usr/share/cluster/cluster.rng**, y el esquema anotado en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (por ejemplo, **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Importante

Algunos procedimientos en este capítulo piden el uso del comando **cman_tool version -r** para propagar un clúster a través de un clúster. El uso de ese comando requiere que **ricci** se esté ejecutando. El uso de **ricci** requiere una contraseña la primera vez que usted interactúa con **ricci** desde una máquina específica. Para obtener información sobre el servicio de **ricci**, consulte la Sección 2.13, “Consideraciones para **ricci**”.

Nota

Los procedimientos en este capítulo pueden incluir comandos específicos para algunas de las herramientas de línea de comandos especificas listadas en el Apéndice E, *Resumen de herramientas de línea de comandos* . Para obtener mayor información sobre todos los comandos y variables, consulte la página de manual para cada herramienta de línea de comandos.

7.1. Tareas de configuración

La configuración de software de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos consta de los siguientes pasos:

1. Creación de un clúster. Consulte la Sección 7.2, “Creación de un archivo de configuración de clúster básico”.
2. Configuración de vallas. Consulte la Sección 7.3, “Configuración de vallas”.
3. Configuración de dominios de conmutación. Consulte la Sección 7.4, “Configuración de dominios de conmutación”.
4. Configuración de servicios de alta disponibilidad. Consulte la Sección 7.5, “Configuración de servicios de alta disponibilidad”.
5. Verificación de una configuración. Consulte la Sección 7.8, “Verificación de una configuración”.

7.2. Creación de un archivo de configuración de clúster básico

Siempre y cuando el hardware de clúster, Red Hat Enterprise Linux y el software de adición de alta disponibilidad estén instalados, podrá crear un archivo de configuración de clúster (**/etc/cluster/cluster.conf**) y empezar a ejecutar la adición de alta disponibilidad. Como punto de partida únicamente, esta sección describe cómo crear un archivo de configuración de clúster de esqueleto sin cercado, dominios de conmutación y servicios de alta disponibilidad. Las siguientes secciones describen cómo configurar esas partes del archivo de configuración.

Importante

Este no es solamente un paso interno para crear un archivo de configuración de clúster; el archivo resultante no tiene ningún cercado y no se considera una configuración compatible.

Los siguientes pasos describen cómo crear y configurar un archivo de configuración de clúster de estructura. Por último, el archivo de configuración para su clúster variará según el número de nodos, el tipo de valla, el tipo, el número de servicios de alta disponibilidad y otros requerimientos específicos.

1. En cualquier nodo en el clúster, cree **/etc/cluster/cluster.conf**, mediante la plantilla del ejemplo en Ejemplo 7.1, “Muestra de **cluster.conf**: Configuración básica”.
2. **(Opcional)** Si está configurando un clúster de dos nodos, puede adicionar la línea al archivo de configuración para que un nodo único pueda mantener cuórum (por ejemplo, si un nodo falla):

   ```
   <cman two_node="1" expected_votes="1"/>
   ```

   Cuando añada o retire la opción **two_node** del archivo **cluster.conf**, debe reiniciar el clúster para que el cambio se efectúe al actualizar la configuración. Para obtener información sobre cómo actualizar y configurar un clúster, consulte la Sección 8.4, “Cómo actualizar una configuración”. Para ver un ejemplo de especificación de la opción **two_node**, consulte el Ejemplo 7.2, “Muestra de **cluster.conf**: Configuración básica de dos nodos”.

3. Especifique el nombre de clúster y el número de versión de configuración mediante los atributos de **cluster**: **name** y **config_version** (consulte el Ejemplo 7.1, "Muestra de **cluster.conf**: Configuración básica" o Ejemplo 7.2, "Muestra de **cluster.conf**: Configuración básica de dos nodos").
4. En la sección **clusternodes**, especifique el nombre de nodos y el ID de nodo de cada nodo mediante los atributos de **clusternode**: **name** y **nodeid**.
5. Guarde **/etc/cluster/cluster.conf**.
6. Valide el archivo con el esquema de clúster (**cluster.rng**) mediante el comando **ccs_config_validate**. Por ejemplo:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Propague el archivo de configuración a **/etc/cluster/** en cada nodo de clúster. Por ejemplo, puede propagar el archivo a otros nodos de clúster mediante el comando **scp**.

Nota

La propagación del archivo de configuración de clúster es necesaria de esta manera la primera vez que se cree el clúster. Una vez que el clúster esté instalado y ejecutándose, el archivo de configuración de clúster puede propagarse con **cman_tool version -r**. Se puede usar el comando **scp** para propagar un archivo de configuración actualizado; sin embargo, el software de clúster debe detenerse en todos los nodos mientras use el comando **scp**. Además, debe ejecutar **ccs_config_validate** si propaga un archivo de configuración actualizado a través de **scp**.

Nota

Aunque hay otros elementos y atributos presentes en el archivo de configuración de muestra, por ejemplo, **fence** y **fencedevices**, no hay necesidad de poblarlos ahora. Procedimientos posteriores en este capítulo proporcionan información acerca de cómo especificar otros elementos y atributos.

8. Inicie el clúster. En cada nodo de clúster ejecute el siguiente comando:

   service cman start

   Por ejemplo:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
```

9. En cualquier nodo de clúster, ejecute **cman_tool nodes** para verificar los nodos que funcionan como miembros en el clúster (representado como "M" en la columna de estatus, "Sts"). Por ejemplo:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

10. Si el clúster está ejecutándose, prosiga a la Sección 7.3, "Configuración de vallas".

Ejemplos de configuración básica

Ejemplo 7.1, “Muestra de `cluster.conf`: Configuración básica” y Ejemplo 7.2, “Muestra de `cluster.conf`: Configuración básica de dos nodos” (para un clúster de dos nodos) cada uno proporciona una muestra básica de un archivo de configuración de clúster como un punto de inicio. Los procedimientos siguientes en este capítulo proporcionan información sobre configuración de cercado y servicios de alta disponibilidad.

Ejemplo 7.1. Muestra de `cluster.conf`: Configuración básica

```
<cluster name="mycluster" config_version="2">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Ejemplo 7.2. Muestra de `cluster.conf`: Configuración básica de dos nodos

```
<cluster name="mycluster" config_version="2">
   <cman two_node="1" expected_votes="1"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

El valor de `consenso` para `totem` en un clúster de dos nodos

Si crea un clúster de dos nodos y no tiene la intención de añadir más nodos al clúster, omita el valor **`consensus`** en la pestaña **`totem`** en el archivo **`cluster.conf`** para que el valor de **`consensus`** se calcule automáticamente. Cuando el valor de **`consensus`** se calcula de esa forma, se aplican las siguientes reglas:

- Si hay dos nodos o menos, el valor de **`consensus`** será (símbolo * 0.2), con un techo de 2.000 ms y un piso de 200 ms.
- Si hay tres o más nodos, el valor de **`consensus`** será (símbolo + 2.000 ms)

Si permite que la herramienta **`cman`** configure su tiempo de espera de consenso en esta forma, entonces al mover de dos a tres (o más) nodos para más tarde, deberá reiniciar el clúster, ya que el tiempo de expiración necesitará cambiar a un valor mayor basado en el tiempo de espera del símbolo.

Si está configurando un clúster de dos nodos e intenta actualizar en el futuro a más de dos nodos, sobrescriba el tiempo de espera del consenso para que el reinicio del clúster no se necesite al pasar de dos a tres nodos (o más). Esto puede realizarse en **cluster.conf** así:

```
<totem token="X" consensus="X + 2000" />
```

Observe que el lector de configuración no calcula X + 2.000 de forma automática. Se debe utilizar un valor de entero en lugar de una ecuación.

La ventaja de usar el espacio de tiempo optimizado de consenso para clúster de dos nodos es que el tiempo de conmutación total se reduce en el caso de dos nodos, ya que el consenso no es una función del tiempo de espera del símbolo.

Observe que para autodetectar dos nodos en **cman**, el número de nodos físicos es lo que importa y no la presencia de la directiva de **two_node=1** en el archivo **cluster.conf**.

7.3. Configuración de vallas

La configuración de vallas consiste en (a) especificar uno o más dispositivos de vallas en un clúster y (b) especificar uno o más métodos de valla para cada nodo (mediante un dispositivo de valla o dispositivos de vallas especificados).

Con base en el tipo de dispositivos de vallas y métodos de vallas requeridos para la configuración, configure **cluster.conf** así:

1. En la sección **fencedevices**, especifique cada dispositivo de vallas, mediante un elemento **fencedevice** y atributos dependientes de dispositivo de vallas. El Ejemplo 7.3, “Dispositivo de vallas APC añadido a **cluster.conf**” presenta un ejemplo de archivo de configuración con una valla APC añadida.
2. En la sección **clusternodes**, dentro del elemento **fence** de cada sección de **clusternode**, especifique cada método de valla del nodo. Especifique el nombre de método de valla, mediante el atributo **method**, **name**. Especifique el dispositivo de vallas para cada método de valla, mediante el elemento **device** y sus atributos, **name** y parámetros específicos de dispositivo de vallas. El Ejemplo 7.4, “Métodos de vallas añadidos a **cluster.conf**” muestra un método de vallas con un dispositivo de valla para cada nodo en el clúster.
3. Para métodos de valla sin energía (es decir, SAN/cercado de almacenamiento), en la sección **clusternodes**, añada una sección **unfence**. De esta manera, garantiza que el nodo cercado no sea reactivado hasta que haya sido reiniciado. Para obtener mayor información sobre cómo quitar la valla a un nodo, consulte la página de manual **fence_node**(8).

   La sección **unfence** no contiene las secciones **method** como la sección de **fence** las contiene. Esta sección contiene referencias directamente de **device**, las cuales copian en espejo las secciones de dispositivo correspondientes a **fence**, con la adición notable de la acción explícita (**action**) de "on" (encendido) o "enable" (activado). El mismo **fencedevice** es referenciado por las líneas de **device fence** y **unfence** y los mismos argumentos por nodo deben repetirse.

   Al especificar el atributo **action** como "encendido " o "habilitado", habilita al nodo durante el reinicio. Ejemplo 7.4, “Métodos de vallas añadidos a **cluster.conf**” y Ejemplo 7.5, “**cluster.conf**: Métodos de vallas múltiples por nodo” incluyen ejemplos de elementos y atributos **unfence**.

   Para obtener mayor información sobre **unfence**, consulte la página de manual **fence_node**.
4. Actualice el atributo **config_version** aumentando su valor (por ejemplo, cambiar de **config_version="2"** a **config_version="3">**).
5. Guarde **/etc/cluster/cluster.conf**.
6. **(Opcional)** Valide el archivo actualizado con el esquema de clúster (**cluster.rng**) ejecutando el comando **ccs_config_validate**. Por ejemplo:

   ```
   [root@example-01 ~]# ccs_config_validate
   Configuration validates
   ```

7. Ejecute el comando **cman_tool version -r** para propagar la configuración a los nodos de clústeres restantes. Así también ejecutará la validación adicional. Es necesario que **ricci** esté en ejecución en cada nodo de clúster para que pueda propagar información actualizada de clúster.
8. Verifique si el archivo de configuración actualizado se ha propagado.

9. Prosiga a la Sección 7.4, “Configuración de dominios de conmutación”.

Si es necesario, puede hacer configuraciones complejas con varios métodos de valla por nodo y con varios dispositivos de valla por el método de vallas. Cuando se especifican varios métodos de vallas por nodo, si falla con el primer método, **fenced**, el demonio de valla, intentará el siguiente método y continúa desplazándose a través de métodos hasta que alguno lo logra.

Algunas veces, para cercar un nodo se requiere desactivar dos rutas de E/S o dos puertos de energía. Esto se realiza al especificar dos o más dispositivos dentro de un método de vallas. **fenced** ejecuta el agente una vez para cada línea de dispositivo de valla; todas deben lograrse para que se considere un cercado correcto.

Para ver configuraciones más complejas, consulte “Ejemplos de configuración de vallas”.

Puede obtener más información sobre configuración de dispositivos de valla específicos desde una página de manual sobre agente de dispositivo de valla (por ejemplo, la página de manual para **fence_apc**). Además, puede obtener mayor información sobre parámetros de cercado en el Apéndice A, *Parámetros de dispositivos de valla*, los agentes de valla en **/usr/sbin/**, el esquema de cluster en **/usr/share/cluster/cluster.rng**, y el esquema anotado en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (por ejemplo, **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Ejemplos de configuración de vallas

Los siguientes ejemplos muestran una configuración sencilla con un método de vallas por nodo y un dispositivo de vallas por método de vallas:

- Ejemplo 7.3, “Dispositivo de vallas APC añadido a **cluster.conf**”
- Ejemplo 7.4, “Métodos de vallas añadidos a **cluster.conf**”

Los siguientes ejemplos muestran configuraciones más complejas:

- Ejemplo 7.5, “**cluster.conf**: Métodos de vallas múltiples por nodo”
- Ejemplo 7.6, “**cluster.conf**: Cercado, múltiples puertos de multirutas”
- Ejemplo 7.7, “**cluster.conf**: Nodos de vallas con dos fuentes de alimentación”

Nota

Los ejemplos en esta sección no son exhaustivos; es decir, puede haber otras formas de configurar vallas según los requerimientos.

Ejemplo 7.3. Dispositivo de vallas APC añadido a `cluster.conf`

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

En este ejemplo, un dispositivo de vallas (**`fencedevice`**) ha sido agregado al elemento **`fencedevices`**, el cual especifica el agente de vallas (**`agent`**) como **`fence_apc`**, la dirección IP (**`ipaddr`**) como **`apc_ip_example`**, el ingreso (**`login`**) como **`login_example`**, el nombre de dispositivo de vallas (**`name`**) como **`apc`**, y la contraseña (**`passwd`**) como **`password_example`**.

Ejemplo 7.4. Métodos de vallas añadidos a `cluster.conf`

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

En este ejemplo, un método de vallas (**`method`**) ha sido agregado a cada nodo. El nombre T del método de vallas (**`name`**) para cada nodo es **`APC`**. El dispositivo (**`device`**) para el método de valla en cada nodo especifica el nombre (**`name`**) como **`apc`** y un único número de puerto de interruptor APC (**`port`**) para cada nodo. Por ejemplo, el número de puerto para nodo-01.example.com es **`1`** (**`port="1"`**). El nombre de dispositivo para nodo (**`device name="apc"`**) señala al dispositivo de valla por el nombre (**`name`**) de **`apc`** en esta línea del elemento **`fencedevices`**: **`fencedevice agent="fence_apc" ipaddr="apc_ip_example" login="login_example" name="apc" passwd="password_example"`**.

Ejemplo 7.5. `cluster.conf`: Métodos de vallas múltiples por nodo

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
            <method name="SAN">
              <device name="sanswitch1" port="11"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="11" action="on"/>
         </unfence
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
            <method name="SAN">
              <device name="sanswitch1" port="12"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="12" action="on"/>
         </unfence
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
            <method name="SAN">
              <device name="sanswitch1" port="13"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="13" action="on"/>
         </unfence
     </clusternode>
   </clusternodes>
   <fencedevices>
        <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Ejemplo 7.6. `cluster.conf`: Cercado, múltiples puertos de multirutas

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="SAN-multi">
              <device name="sanswitch1" port="11"/>
              <device name="sanswitch2" port="11"/>
            </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="11" action="on"/>
             <device name="sanswitch2" port="11" action="on"/>
         </unfence
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="SAN-multi">
              <device name="sanswitch1" port="12"/>
              <device name="sanswitch2" port="12"/>
            </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="12" action="on"/>
             <device name="sanswitch2" port="12" action="on"/>
         </unfence
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="SAN-multi">
              <device name="sanswitch1" port="13"/>
              <device name="sanswitch2" port="13"/>
            </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="13" action="on"/>
             <device name="sanswitch2" port="13" action="on"/>
         </unfence
     </clusternode>
   </clusternodes>
   <fencedevices>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch2" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Ejemplo 7.7. `cluster.conf`: Nodos de vallas con dos fuentes de alimentación

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="1"action="off"/>
              <device name="apc2" port="1"action="off"/>
              <device name="apc1" port="1"action="on"/>
              <device name="apc2" port="1"action="on"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="2"action="off"/>
              <device name="apc2" port="2"action="off"/>
              <device name="apc1" port="2"action="on"/>
              <device name="apc2" port="2"action="on"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="3"action="off"/>
              <device name="apc2" port="3"action="off"/>
              <device name="apc1" port="3"action="on"/>
              <device name="apc2" port="3"action="on"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
       <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc1" passwd="password_example"/>
       <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc2" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Cuando se utilizan interruptores para cercar nodos con dos fuentes de alimentación, los agentes deben indicarle que apague ambos puertos antes de restaurar la energía a cualquiera de los puertos. El comportamiento predeterminado off-on del agente podría hacer que la energía nunca se desactive de forma total para el nodo.

7.4. Configuración de dominios de conmutación

Un dominio de conmutación es un subconjunto con nombre de nodos de clúster elegibles para ejecutar un servicio de clúster en caso de una falla de nodo. Un dominio de conmutación puede tener las siguientes características:

- Sin restricciones — Le permite especificar que un subconjunto de miembros se prefiera, pero que el servicio de clúster asignado a este dominio pueda ejecutarse en cualquier miembro disponible.
- Restringido — Le permite restringir los miembros que pueden ejecutar un servicio de clúster particular. Si ninguno de los miembros en un dominio de conmutación restringido está disponible, el servicio de clúster no puede iniciarse (ya sea en forma manual o por el software de clúster).
- Desordenado — Cuando el servicio de clúster se asigna a un dominio de conmutación desordenado, el miembro en el que se ejecuta el servicio de clúster es elegido entre los

miembros de dominio de conmutación sin ningún orden de prioridad.

- Ordenado — Le permite especificar un orden de preferencia entre los miembros de un dominio de conmutación. Los dominios de conmutación seleccionan el nodo con el número de prioridad inferior en primer lugar. Es decir, el nodo en un dominio de conmutación con un número de prioridad de "1" especifica la máxima prioridad, y por lo tanto, es el nodo preferido en un dominio de conmutación. Después de ese nodo, el siguiente nodo preferido sería el nodo con el siguiente número de prioridad más alto y así sucesivamente.
- Recuperación — Le permite especificar si un servicio en el dominio de conmutación debe recuperar al nodo que originalmente estaba ejecutándose antes de que ese nodo falle. La configuración de esta característica es útil en circunstancias donde un nodo repetidamente falla y hace parte de un dominio de conmutación ordenado. En esas circunstancias, si un nodo es el nodo preferido en un dominio de conmutación, es posible que un servicio se conmute o se recupere repetidas veces entre el nodo preferido y otro nodo, lo cual repercute gravemente en el rendimiento.

Nota

La funcionalidad de recuperación de fallos se aplica únicamente si la configuración de conmutación ordenada está configurada.

Nota

El cambio de una configuración de dominio de conmutación no se efectúa en servicios que se están ejecutando.

Nota

Los dominios de conmutación *no* se requieren para operación.

Por defecto, los dominios de conmutación son desordenados y sin restricciones.

En un clúster con varios miembros, si utiliza un dominio de conmutación restringido puede minimizar la labor de configuración del clúster para ejecutar un servicio de clúster (como **httpd**), el cual requiere que establezca la configuración idéntica en todos los miembros que ejecuten el servicio de clúster. En lugar de configurar todo el clúster para que ejecute el servicio de clúster, únicamente configure los miembros del dominio de conmutación restringido asociados con el servicio de clúster.

Nota

Para configurar a un miembro preferido, puede crear un dominio de conmutación sin restricciones que consta de un único miembro del clúster. Al hacer esto, el servicio de clúster se ejecutará en ese miembro del clúster principalmente (el miembro preferido), pero permitirá que el servicio de clúster recupere fallas de cualquiera de los otros miembros.

Para configurar un dominio de conmutación, use los siguientes procedimientos:

1. Abra **/etc/cluster/cluster.conf** en cualquier nodo en el clúster.
2. Añada la siguiente sección de estructura dentro del elemento **rm** para cada dominio de conmutación que se va a utilizar:

```
        <failoverdomains>
            <failoverdomain name="" nofailback="" ordered=""
restricted="">
                <failoverdomainnode name="" priority=""/>
                <failoverdomainnode name="" priority=""/>
                <failoverdomainnode name="" priority=""/>
            </failoverdomain>
        </failoverdomains>
```

Nota

El número de atributos **failoverdomainnode** depende del número de nodos en el dominio de conmutación. La estructura de la sección **failoverdomain** en el texto anterior muestra tres elementos **failoverdomainnode** (sin nombres de nodos especificados), lo cual significa que hay tres nodos en el dominio de conmutación.

3. En la sección **failoverdomain**, proporcione los valores para los elementos y atributos. Para obtener descripciones de los elementos y atributos, consulte la sección *failoverdomain* del esquema de cluster anotado. El esquema de cluster anotado está disponible en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (por ejemplo, **/usr/share/doc/cman-3.0.12/cluster_conf.html**) en cualquiera de los nodos de cluster. Para ver un ejemplo de una sección **failoverdomains**, consulte el Ejemplo 7.8, “Un dominio de conmutación de fallas para **cluster.conf**”.
4. Actualice el atributo **config_version** aumentando su valor (por ejemplo, cambiar de **config_version="2"** a **config_version="3">**).
5. Guarde **/etc/cluster/cluster.conf**.
6. **(Opcional)** Valide el archivo con el esquema de cluster (**cluster.rng**) al ejecutar el comando **ccs_config_validate**. Por ejemplo:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Ejecute el comando **cman_tool version -r** para propagar la configuración al resto de nodos de clúster.
8. Prosiga a la Sección 7.5, “Configuración de servicios de alta disponibilidad”.

El Ejemplo 7.8, “Un dominio de conmutación de fallas para **cluster.conf**” muestra una configuración con un dominio de conmutación ordenado, sin restricciones.

Ejemplo 7.8. Un dominio de conmutación de fallas para `cluster.conf`

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
          <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
              <failoverdomainnode name="node-01.example.com" priority="1"/>
              <failoverdomainnode name="node-02.example.com" priority="2"/>
              <failoverdomainnode name="node-03.example.com" priority="3"/>
          </failoverdomain>
       </failoverdomains>
   </rm>
</cluster>
```

La sección **`failoverdomains`** contiene una sección **`failoverdomain`** para cada dominio de conmutación en el cluster. Este ejemplo tiene un dominio de conmutación . En la línea **`failoverdomain`**, el nombre (**`name`**) se especifica como **`example_pri`**. Además, especifica sin recuperación (**`failback="0"`**), esa conmutación es ordenada (**`ordered="1"`**), y ese dominio de conmutación es sin restricciones (**`restricted="0"`**).

7.5. Configuración de servicios de alta disponibilidad

La configuración de servicios de alta disponibilidad (HA) consta de recursos de configuración y de la asignación a servicios.

Las siguientes secciones describen cómo editar **`/etc/cluster/cluster.conf`** para añadir recursos y servicios.

- Sección 7.5.1, “Adición de recursos de clúster”
- Sección 7.5.2, “Adición de un servicio de clúster al clúster”

Importante

Puede haber una amplia gama de configuraciones posibles con los servicios y recursos de alta disponibilidad. Para entender mejor los parámetros de recursos y la conducta de recursos, consulte el Apéndice B, *Parámetros de recursos de alta disponibilidad* y Apéndice C, *Comportamiento de recursos de alta disponibilidad*. Para rendimiento óptimo y para asegurarse de que su configuración tiene soporte, contacte a un representante autorizado de Red Hat.

7.5.1. Adición de recursos de clúster

Puede configurar dos tipos de recursos:

- Globales — Recursos que están disponibles para cualquier servicio en el clúster. Estos recursos se configuran en la sección **resources** del archivo de configuración (dentro del elemento **rm**).
- Servicio específico — Recursos que están disponibles para un servicio únicamente. Estos recursos se configuran en cada sección **service** del archivo de configuración (dentro del elemento **rm**).

Esta sección describe cómo añadir un recurso global. Para ver procedimientos sobre configuración de servicio de recursos específicos, consulte la Sección 7.5.2, "Adición de un servicio de clúster al clúster".

Para añadir un recurso de clúster global, siga los siguientes pasos en esta sección.

1. Abra **/etc/cluster/cluster.conf** en cualquier nodo en el clúster.
2. Añada una sección de **resources** dentro del elemento **rm**. Por ejemplo:

```
<rm>
    <resources>

    </resources>
</rm>
```

3. Pueblelo con recursos de acuerdo con los servicios que desea crear. Por ejemplo, aquí están los recursos que se deben utilizar en un servicio de Apache. Ellos constan de un recurso de sistema de archivos (**fs**), un recurso de IP (**ip**) y un recurso de Apache (**apache**).

```
<rm>
    <resources>
       <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
       <ip address="127.143.131.100" monitor_link="yes"
sleeptime="10"/>
       <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
    </resources>
</rm>
```

   Ejemplo 7.9, "Archivo **cluster.conf** con recursos agregados" muestra un archivo **cluster.conf** con la sección de **resources** añadida.
4. Actualice el atributo de **config_version** al incrementar su valor (por ejemplo, cambiando de **config_version="2"** a **config_version="3"**).
5. Guarde **/etc/cluster/cluster.conf**.
6. **(Opcional)** Valide el archivo con el esquema de cluster (**cluster.rng**) al ejecutar el comando **ccs_config_validate**. Por ejemplo:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Ejecute el comando **cman_tool version -r** para propagar la configuración al resto de nodos de clúster.
8. Verifique si el archivo de configuración actualizado se ha propagado.
9. Prosiga a la Sección 7.5.2, "Adición de un servicio de clúster al clúster".

Ejemplo 7.9. Archivo `cluster.conf` con recursos agregados

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
               <failoverdomainnode name="node-01.example.com" priority="1"/>
               <failoverdomainnode name="node-02.example.com" priority="2"/>
               <failoverdomainnode name="node-03.example.com" priority="3"/>
           </failoverdomain>
       </failoverdomains>
       <resources>
           <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
           <ip address="127.143.131.100" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>

   </rm>
</cluster>
```

7.5.2. Adición de un servicio de clúster al clúster

Para añadir un servicio de clúster al clúster, sigan los siguientes pasos en esta sección.

1. Abra **`/etc/cluster/cluster.conf`** en cualquier nodo en el clúster.
2. Añada la sección **`service`** dentro del elemento **`rm`** para cada servicio. Por ejemplo:

```
       <rm>
           <service autostart="1" domain="" exclusive="0" name=""
   recovery="restart">

           </service>
       </rm>
```

3. Configure los siguientes parámetros (atributos) en el elemento de **`service`**:
   - **`autostart`** — Especifica si autoinicia el servicio o no, cuando el clúster inicie. Use

'1' para activar y '0' para desactivar; se predetermina como activado.

- **domain** — Especifica un dominio de conmutación (si se requiere).
- **exclusive** — Especifica una política en la que el servicio solamente se ejecuta en nodos que no tienen otros servicios ejecutándose en ellos.
- **recovery** — Especifica una política de recuperación para el servicio. Las opciones deben reubicar, reiniciar, desactivar, o reiniciar-desactivar el servicio.

4. Según el tipo de recursos que desee utilizar, pueble el servicio con servicio de recursos globales o específicos

   Por ejemplo, el siguiente es un servicio de Apache que usa recursos globales:

```
    <rm>
        <resources>
                <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
                <ip address="127.143.131.100" monitor_link="on"
sleeptime="10"/>
                <apache config_file="conf/httpd.conf"
name="example_server" server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>
        <service autostart="1" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
                <fs ref="web_fs"/>
                <ip ref="127.143.131.100"/>
                <apache ref="example_server"/>
        </service>
    </rm>
```

   Por ejemplo, el siguiente es un servicio de Apache que utiliza un servicio de recursos específicos:

```
    <rm>
        <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
                <fs name="web_fs2" device="/dev/sdd3"
mountpoint="/var/www2" fstype="ext3"/>
                <ip address="127.143.131.101" monitor_link="yes"
sleeptime="10"/>
                <apache config_file="conf/httpd.conf"
name="example_server2" server_root="/etc/httpd" shutdown_wait="0"/>
        </service>
    </rm>
```

   El Ejemplo 7.10, "**cluster.conf** con servicios añadidos: Uno mediante recursos globales y otro mediante recursos de servicio específico" muestra un archivo **cluster.conf** con dos servicios:

   - **example_apache** — Este servicio usa recursos globales **web_fs**, **127.143.131.100**, y **example_server**.
   - **example_apache2** — Este servicio usa servicio de recursos específicos **web_fs2**, **127.143.131.101**, y **example_server2**.

5. Actualice el atributo **config_version** aumentando su valor (por ejemplo, cambiar de **config_version="2"** a **config_version="3">**).
6. Guarde **/etc/cluster/cluster.conf**.
7. **(Opcional)** Valide el archivo actualizado con el esquema de clúster (**cluster.rng**) ejecutando el comando **ccs_config_validate**. Por ejemplo:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

8. Ejecute el comando **cman_tool version -r** para propagar la configuración al resto de nodos de clúster.
9. Verifique si el archivo de configuración actualizado se ha propagado.
10. Prosiga a la Sección 7.8, "Verificación de una configuración".

Ejemplo 7.10. `cluster.conf` con servicios añadidos: Uno mediante recursos globales y otro mediante recursos de servicio específico

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
          <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
              <failoverdomainnode name="node-01.example.com" priority="1"/>
              <failoverdomainnode name="node-02.example.com" priority="2"/>
              <failoverdomainnode name="node-03.example.com" priority="3"/>
          </failoverdomain>
       </failoverdomains>
       <resources>
          <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
          <ip address="127.143.131.100" monitor_link="yes" sleeptime="10"/>
          <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
       </resources>
       <service autostart="1" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
          <fs ref="web_fs"/>
          <ip ref="127.143.131.100"/>
          <apache ref="example_server"/>
       </service>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
          <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www2"
fstype="ext3"/>
          <ip address="127.143.131.101" monitor_link="yes" sleeptime="10"/>
          <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
       </service>
   </rm>
</cluster>
```

7.6. Cómo configura el protocolo de anillos redundantes

A partir de Red Hat Enterprise Linux 6.4, la adición de alta disponibilidad de Red Hat soporta la configuración redundante del protocolo de anillos redundantes.

Al configurar un sistema para usar un protocolo de anillo redundante, usted debe tener en cuenta lo siguiente:

- No especifique más de dos anillos.
- Cada anillo debe utilizar el mismo protocolo; no mezcle IPv4 con IPv6.
- Si es necesario, especifique manualmente una dirección mutidifusión para un segundo anillo. Si especifica una dirección multidifusión para el segundo anillo, ya sea la dirección multidifusión o el puerto alterno debe ser diferente a la dirección multidifusión para el primer anillo. Si usted no especifica una dirección multidifusión alterna, el sistema utilizará automáticamente una dirección multidifusión diferente para el segundo anillo.

  Si especifica un puerto alterno, los números de puerto del primer anillo y del segundo anillo deben diferir en al menos dos, ya que el sistema utiliza los puertos 'Port' y 'Port -1' para realizar operaciones.
- No utilice dos interfaces diferentes en la misma subred.
- En general, es una buena práctica configurar el protocolo de anillos redundantes en dos NIC y dos interruptores diferentes, en caso de que un NIC o interruptor falle.
- No use el comando **`ifdown`** ni el comando **`service network stop`** para simular la interrupción de red. Al hacerlo destruirá todo el clúster y deberá reiniciar todos los nodos en el clúster que va a recuperar.
- No utilice **`NetworkManager`**, ya que ejecutará el comando **`ifdown`** si el cable está desconecto.
- Cuando un nodo de un NIC falla, todo el anillo se marcará como errado.
- Ninguna intervención manual se requiere para recuperar un anillo que haya fallado. Para recuperar, solo necesita corregir la razón de origen de la falla, como por ejemplo, un NIC o un interruptor que hayan fallado.

Para configurar una segunda interfaz de red para que use protocolo de anillos redundantes, añada un componente **`altname`** a la sección **`clusternode`** del archivo de configuración **`cluster.conf`**. Para configurar **`altname`**, debe especificar un atributo **`name`** para indicar un segundo nombre de host o dirección IP para el nodo.

El siguiente ejemplo especifica **`clusternet-node1-eth2`** como el nombre para el nodo de clúster alterno **`clusternet-node1-eth1`**.

```
<cluster name="mycluster" config_version="3" >
  <logging debug="on"/>
  <clusternodes>
    <clusternode name="clusternet-node1-eth1" votes="1" nodeid="1">
      <fence>
        <method name="single">
          <device name="xvm" domain="clusternet-node1"/>
        </method>
      </fence>
      <altname name="clusternet-node1-eth2"/>
    </clusternode>
```

La sección **`altname`** dentro del bloque **`clusternode`** no depende de la ubicación. Puede estar antes o después de la sección de **`fence`**. No especifique más de un componente **`altname`** para un nodo de clúster, de lo contrarió, el sistema fallará en el inicio.

También, puede especificar de forma manual una dirección multidifusión, un puerto, un TTL para el segundo anillo incluido el componente **`altmulticast`** en la sección **`cman`** del archivo de configuración **`cluster.conf`**. El componente **`altmulticast`** acepta un parámetro **`addr`**, un parámetro **`port`**, y un parámetro **`ttl`**.

El siguiente ejemplo muestra la sección **`cman`** de un archivo de configuración de un clúster que establece una dirección multidifusión, un puerto y TTL para el segundo anillo.

```
<cman>
   <multicast addr="239.192.99.73" port="666" ttl="2"/>
   <altmulticast addr="239.192.99.88" port="888" ttl="3"/>
</cman>
```

7.7. Configuración de opciones de depuración

Puede activar la depuración para todos los demonios en un clúster o habilitar el registro para procesamiento de clúster específico.

Para habilitar la depuración para todos los demonios, añada lo siguiente al **/etc/cluster/cluster.conf**. Por defecto, el registro se dirige al archivo **/var/log/cluster/*daemon*.log**.

```
<cluster config_version="7" name="rh6cluster">
  <logging debug="on"/>
   ...
</cluster>
```

Para habilitar la depuración en los procesos de cluster, añada las siguientes líneas al archivo **/etc/cluster/cluster.conf**. La configuración de registro por demonio sobrescribe los parámetros globales.

```
<cluster config_version="7" name="rh6cluster">
   ...
  <logging>
       <!-- turning on per-subsystem debug logging -->
       <logging_daemon name="corosync" debug="on" />
       <logging_daemon name="fenced" debug="on" />
       <logging_daemon name="qdiskd" debug="on" />
       <logging_daemon name="rgmanager" debug="on" />
       <logging_daemon name="dlm_controld" debug="on" />
       <logging_daemon name="gfs_controld" debug="on" />
  </logging>
   ...
</cluster>
```

Para obtener un listado de los demonios de registro, con los cuales puede habilitar el registro así como las opciones de registro adicionales que se pueden configurar para el registro global y para el registro por demonio, consulte la página de manual **cluster.conf**(5).

7.8. Verificación de una configuración

Cuando haya creado su archivo de configuración de clúster, verifique si está ejecutándose correctamente al realizar los siguientes pasos:

1. En cada nodo, reinicie el software de clúster. Esa acción asegura que cualquier adición de configuración que se verifica solamente en el tiempo de inicio se incluye en la configuración que está ejecutándose. Puede iniciar el software de clúster con **service cman restart**. Por ejemplo:

```
[root@example-01 ~]# service cman restart
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
```

2. Ejecute **service clvmd start**, si CLVM está siendo utilizada para crear volúmenes de cluster. Por ejemplo:

```
[root@example-01 ~]# service clvmd start
Activating VGs:                                            [  OK  ]
```

3. Ejecute **service gfs2 start**, si está utilizando Red Hat GFS2. Por ejemplo:

```
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
```

4. Ejecute **service rgmanager start** mediante los servicios de alta disponibilidad (HA). Por ejemplo:

```
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
```

5. En cualquier nodo de clúster, ejecute **cman_tool nodes** para verificar los nodos que funcionan como miembros en el clúster (representado como "M" en la columna de estatus, "Sts"). Por ejemplo:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

6. En cualquier nodo, con la herramienta **clustat**, verifique si los servicios de alta disponibilidad se están ejecutando como esperado. Además, **clustat** muestra el estatus de los nodos de clúster. Por ejemplo:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    -----
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)                         disabled
```

7. Si el clúster está ejecutándose como se esperaba, habrá terminado de crear un archivo de configuración. Puede administrar el clúster con las herramientas de línea de comandos descritas en el Capítulo 8, *Administración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos*.

Capítulo 8. Administración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos

8.1. Iniciar y parar el software de clúster
8.1.1. Cómo iniciar software de clúster
8.1.2. Cómo detener el software de clúster

8.2. Borrar o añadir un nodo
8.2.1. Cómo borrar un nodo de un clúster
8.2.2. Adición de un nodo a un cluster
8.2.3. Ejemplos de configuraciones de tres y dos nodos.

8.3. Administrar servicios de alta disponibilidad
8.3.1. Cómo desplegar el estatus de servicio de alta disponibilidad con `clustat`
8.3.2. Cómo administrar servicios de alta disponibilidad con `clusvcadm`

8.4. Cómo actualizar una configuración
8.4.1. Cómo actualizar una configuración con `cman_tool version -r`
8.4.2. Actualizar y configurar mediante `scp`

Este capítulo describe varias tareas administrativas para el manejo de adición de alta disponibilidad de Red Hat y consta de la siguientes secciones:

- Sección 8.1, “Iniciar y parar el software de clúster”
- Sección 8.2, “Borrar o añadir un nodo”
- Sección 8.3, “Administrar servicios de alta disponibilidad”
- Sección 8.4, “Cómo actualizar una configuración”

Importante

Asegúrese de que la implementación de la adición de alta disponibilidad de Red Hat satisfaga sus necesidades y pueda estar soportada. Consulte a un representante autorizado de Red Hat para verificar su configuración antes de implementarla. Además, disponga de un periodo de quemado de configuración para probar modos de fallas.

Importante

Este capítulo hace referencia a los elementos y atributos de **`cluster.conf`** más utilizados. Para obtener una lista y descripción completa de **`cluster.conf`**, consulte el esquema de cluster en **`/usr/share/cluster/cluster.rng`**, y el esquema anotado en **`/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html`** (por ejemplo, **`/usr/share/doc/cman-3.0.12/cluster_conf.html`**).

Importante

Algunos procedimientos en este capítulo piden el uso del comando **`cman_tool version -r`** para propagar un clúster a través de un clúster. El uso de ese comando requiere que **`ricci`** se esté ejecutando.

Nota

Los procedimientos en este capítulo, pueden incluir comandos específicos para algunas de las herramientas de línea de comandos especificas listadas en el Apéndice E, *Resumen de herramientas de línea de comandos* . Para obtener mayor información sobre todos los comandos y variables, consulte la página de manual para cada herramienta de línea de comandos.

8.1. Iniciar y parar el software de clúster

Puede iniciar o parar un software de clúster en un nodo según la Sección 8.1.1, “Cómo iniciar software de clúster” y la Sección 8.1.2, “Cómo detener el software de clúster”. El inicio de software de clúster en un nodo hace que se conecte al clúster; al detener el software de clúster en un nodo hace que abandone el clúster.

8.1.1. Cómo iniciar software de clúster

Para iniciar el software de clúster en un nodo, escriba los siguientes comandos en este orden:

1. **`service cman start`**
2. **`service clvmd start`**, si se ha utilizado CLVM para crear volúmenes en clúster
3. **`service gfs2 start`**, si está usando Red Hat GFS2
4. **`service rgmanager start`**, si está utilizando servicios de alta disponibilidad (**`rgmanager`**).

Por ejemplo:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example" now active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

8.1.2. Cómo detener el software de clúster

Para detener el software de clúster en un nodo, escriba los siguientes comandos en este orden:

1. **`service rgmanager stop`**, si está utilizando servicios de alta disponibilidad (**`rgmanager`**).
2. **`service gfs2 stop`**, si está utilizando Red Hat GFS2
3. **`umount -at gfs2`**, si está utilizando Red Hat GFS2 junto con **`rgmanager`**, para asegurarse que los archivos de GFS2 montados durante el inicio de **`rgmanager`** (pero no desmontados durante el apagado) sean también desmontados.
4. **`service clvmd stop`**, si CLVM se ha utilizado para crear volúmenes en cluster
5. **`service cman stop`**

Por ejemplo:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# umount -at gfs2
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

Nota

Al detener el software de clúster en un nodo los servicios de alta Disponibilidad se conmutan a otro nodo. Como una alternativa, puede reubicar o migrar servicios de alta Disponibilidad a otro nodo antes de detener el software de clúster. Para obtener información sobre manejo de servicios de alta disponibilidad, consulte la Sección 8.3, “Administrar servicios de alta disponibilidad”.

8.2. Borrar o añadir un nodo

Esta sección describe cómo borrar un nodo desde un clúster y añadir un nodo a un clúster. Puede borrar un nodo desde un clúster según la Sección 8.2.1, “Cómo borrar un nodo de un clúster”; puede añadir un nodo a un clúster según la Sección 8.2.2, “Adición de un nodo a un cluster”.

8.2.1. Cómo borrar un nodo de un clúster

Para borrar un nodo de un clúster, apague el software de clúster en el nodo que va a ser borrado y actualice la configuración de clúster para reflejar el cambio.

Importante

Al borrar un nodo del clúster se produce una transición de más de dos nodos a dos nodos, debe reiniciar el software de clúster en cada nodo después de actualizar el archivo de configuración de clúster.

Para borrar un nodo de un clúster, realice los siguientes pasos:

1. En cualquier nodo, use la herramienta **clusvcadm** para reubicar, migrar, o parar cada servicio de alta disponibilidad que se esté ejecutando en el nodo que se está eliminando del clúster. Para obtener información sobre el uso de **clusvcadm**, consulte la Sección 8.3, “Administrar servicios de alta disponibilidad”.
2. En el nodo que va a ser eliminado del clúster, pare el software de clúster de acuerdo con la Sección 8.1.2, “Cómo detener el software de clúster”. Por ejemplo:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

3. En cualquier nodo en el clúster, edite **/etc/cluster/cluster.conf** para eliminar la sección **clusternode** del nodo que va a ser seleccionado. En el Ejemplo 8.1, "Configuración de clúster de tres nodos", si se supone que node-03.example.com va a ser eliminado, entonces borre la sección **clusternode** para ese nodo. Si al eliminar un nodo (o nodos) hace que el cluster tenga dos nodos, puede añadir la siguiente línea al archivo de configuración para permitir a un nodo único mantener cuórum (por ejemplo, si un nodo falla):

   <cman two_node="1" expected_votes="1"/>

   Consulte la Sección 8.2.3, "Ejemplos de configuraciones de tres y dos nodos." para comparar entre una configuración de tres nodos y una de dos nodos.
4. Actualice el atributo **config_version** aumentando su valor (por ejemplo, cambiar de **config_version="2"** a **config_version="3">**).
5. Guarde **/etc/cluster/cluster.conf**.
6. **(Opcional)** Valide el archivo actualizado con el esquema de clúster (**cluster.rng**) ejecutando el comando **ccs_config_validate**. Por ejemplo:

   ```
   [root@example-01 ~]# ccs_config_validate
   Configuration validates
   ```

7. Ejecute el comando **cman_tool version -r** para propagar la configuración al resto de nodos de clúster.
8. Verifique si el archivo de configuración actualizado se ha propagado.
9. Si la cuenta de nodo del clúster ha pasado de más de dos nodos a dos nodos, debe reiniciar el software de clúster así:
   a. En cada nodo, pare el software de clúster de acuerdo con la Sección 8.1.2, "Cómo detener el software de clúster". Por ejemplo:

      ```
      [root@example-01 ~]# service rgmanager stop
      Stopping Cluster Service Manager:                          [  OK  ]
      [root@example-01 ~]# service gfs2 stop
      Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
      Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
      [root@example-01 ~]# service clvmd stop
      Signaling clvmd to exit                                    [  OK  ]
      clvmd terminated                                           [  OK  ]
      [root@example-01 ~]# service cman stop
      Stopping cluster:
         Leaving fence domain...                                 [  OK  ]
         Stopping gfs_controld...                                [  OK  ]
         Stopping dlm_controld...                                [  OK  ]
         Stopping fenced...                                      [  OK  ]
         Stopping cman...                                        [  OK  ]
         Waiting for corosync to shutdown:                       [  OK  ]
         Unloading kernel modules...                             [  OK  ]
         Unmounting configfs...                                  [  OK  ]
      [root@example-01 ~]#
      ```

   b. En cada nodo, inicie el software de clúster de acuerdo con la Sección 8.1.1, "Cómo

iniciar software de clúster". Por ejemplo:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example"
now active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

c. En cualquier nodo de clúster, ejecute **cman_tool nodes** para verificar los nodos que funcionan como miembros en el cluster (representado como "M" en la columna de estatus, "Sts"). Por ejemplo:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
```

d. En cualquier nodo, mediante la herramienta **clustat**, verifique si los servicios de alta disponibilidad se están ejecutando como esperado. Además, **clustat** muestra el estatus de los nodos de clúster. Por ejemplo:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local,
rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    -----
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)
disabled
```

8.2.2. Adición de un nodo a un cluster

Adicionar un nodo a un clúster consiste en actualizar la configuración de clúster, propagar la configuración actualizada para el nodo añadido, e iniciar el software de clúster en ese nodo. Para añadir un nodo a un clúster, realice los siguientes pasos:

1. En cualquier nodo en el clúster, edite **/etc/cluster/cluster.conf** para añadir una sección **clusternode** para el nodo que se va a añadir. En el Ejemplo 8.2, "Configuración de clúster de dos nodos", si node-03.example.com se supone que va a ser añadido, entonces añada una sección **clusternode** para ese nodo. Si al añadir un nodo (o nodos) el cluster pasa de un clúster de dos nodos a un clúster de tres nodos o más, elimine los siguientes atributos **cman** de **/etc/cluster/cluster.conf**:
   - **cman two_node="1"**

- **expected_votes="1"**

Consulte la Sección 8.2.3, “Ejemplos de configuraciones de tres y dos nodos.” para comparar entre una configuración de tres nodos y una de dos nodos.

2. Actualice el atributo **config_version** aumentando su valor (por ejemplo, cambiar de **config_version="2"** a **config_version="3">**).
3. Guarde **/etc/cluster/cluster.conf**.
4. **(Opcional)** Valide el archivo actualizado con el esquema de clúster (**cluster.rng**) ejecutando el comando **ccs_config_validate**. Por ejemplo:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

5. Ejecute el comando **cman_tool version -r** para propagar la configuración al resto de nodos de clúster.
6. Verifique si el archivo de configuración actualizado se ha propagado.
7. Propague el archivo de configuración a **/etc/cluster/** en cada nodo para que sea agregado al cluster. Por ejemplo, use el comando **scp** para enviar el archivo de configuración a cada nodo que va a ser añadido al cluster.
8. Si la cuenta de nodo del clúster ha pasado de dos nodos a más de dos nodos, debe reiniciar el software de clúster en los nodos de clúster existentes así:
   a. En cada nodo, pare el software de clúster de acuerdo con la Sección 8.1.2, “Cómo detener el software de clúster”. Por ejemplo:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

   b. En cada nodo, inicie el software de clúster de acuerdo con la Sección 8.1.1, “Cómo iniciar software de clúster”. Por ejemplo:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example"
now active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

9. En cada nodo que va a ser agregado al clúster, inicie el software de clúster según la Sección 8.1.1, “Cómo iniciar software de clúster”. Por ejemplo:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example" now
active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]

[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

10. En cualquier nodo, al usar la herramienta **clustat**, verifique si cada nodo añadido está ejecutándose y parte del clúster. Por ejemplo:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    -----
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)                         disabled
```

Para obtener información sobre el uso de **clustat**, consulte la Sección 8.3, “Administrar servicios de alta disponibilidad”.

Además, puede usar **cman_tool status** para verificar votos de nodos, cuenta de nodos y cuenta de cuórum.

```
[root@example-01 ~]#cman_tool status
Version: 6.2.0
Config Version: 19
Cluster Name: mycluster
Cluster Id: 3794
Cluster Member: Yes
Cluster Generation: 548
Membership state: Cluster-Member
Nodes: 3
Expected votes: 3
Total votes: 3
Node votes: 1
Quorum: 2
Active subsystems: 9
Flags:
Ports Bound: 0 11 177
Node name: node-01.example.com
Node ID: 3
Multicast addresses: 239.192.14.224
Node addresses: 10.15.90.58
```

11. En cualquier nodo, puede usar la herramienta **clusvcadm** para migrar o reubicar un servicio en ejecución para el nuevo nodo recién conectado. También, puede habilitar cualquier servicio inactivo. Para obtener información sobre el uso de **clusvcadm**, consulte la Sección 8.3, “Administrar servicios de alta disponibilidad”

8.2.3. Ejemplos de configuraciones de tres y dos nodos.

Consulte los ejemplos a continuación para comparar entre la configuración de tres nodos y de dos nodos.

Ejemplo 8.1. Configuración de clúster de tres nodos

```
<cluster name="mycluster" config_version="3">
   <cman/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
          <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
              <failoverdomainnode name="node-01.example.com" priority="1"/>
              <failoverdomainnode name="node-02.example.com" priority="2"/>
              <failoverdomainnode name="node-03.example.com" priority="3"/>
          </failoverdomain>
       </failoverdomains>
       <resources>
          <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
          <ip address="127.143.131.100" monitor_link="yes" sleeptime="10"/>
          <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
       </resources>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
          <fs ref="web_fs"/>
          <ip ref="127.143.131.100"/>
          <apache ref="example_server"/>
       </service>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
          <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www"
fstype="ext3"/>
          <ip address="127.143.131.101" monitor_link="yes" sleeptime="10"/>
          <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
       </service>
   </rm>
</cluster>
```

Ejemplo 8.2. Configuración de clúster de dos nodos

```
<cluster name="mycluster" config_version="3">
   <cman two_node="1" expected_votes="1"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
               <failoverdomainnode name="node-01.example.com" priority="1"/>
               <failoverdomainnode name="node-02.example.com" priority="2"/>
           </failoverdomain>
       </failoverdomains>
       <resources>
           <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
           <ip address="127.143.131.100" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
       </resources>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
           <fs ref="web_fs"/>
           <ip ref="127.143.131.100"/>
           <apache ref="example_server"/>
       </service>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
           <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www"
fstype="ext3"/>
           <ip address="127.143.131.101" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
       </service>
   </rm>
</cluster>
```

8.3. Administrar servicios de alta disponibilidad

Puede manejar servicios de alta disponibilidad mediante la **Herramienta de estatus de clúster**, **`clustat`**, y la **Herramienta de administración de servicios de usuario de clúster**, **`clusvcadm`**. **`clustat`** muestra el estatus de un clúster y **`clusvcadm`** proporciona los medios para administrar los servicios de alta disponibilidad.

Esta sección proporciona la información básica sobre manejo de servicios de alta disponibilidad mediante **`clustat`** y **`clusvcadm`**, consta de las siguientes subpartes:

- Sección 8.3.1, “Cómo desplegar el estatus de servicio de alta disponibilidad con **`clustat`**”

- Sección 8.3.2, “Cómo administrar servicios de alta disponibilidad con **clusvcadm**”

8.3.1. Cómo desplegar el estatus de servicio de alta disponibilidad con clustat

clustat muestra el estatus global de clúster. Muestra la información de membresía, vista de cuórum, el estado de todos los servicios de alta disponibilidad e indica el nodo en que **clustat** se está ejecutando (Local). La Tabla 8.1, “Estatus de servicios” describe los estados de los servicios y se muestran al ejecutar **clustat**. Ejemplo 8.3, “Pantalla **clustat** ” muestra un ejemplo de una pantalla de **clustat**. Para obtener información más detallada sobre ejecución del comando **clustat**, consulte la página de manual **clustat**.

Tabla 8.1. Estatus de servicios

Estatus de servicios	Descripción
Iniciado	Los recursos del servicio están configurados y disponibles en el sistema de clúster que posee el servicio.
Recuperación	El servicio está pendiente de iniciar en otro nodo.
Inhabilitado	El servicio se ha inhabilitado y no tiene un propietario asignado. Un servicio inhabilitado nunca es reiniciado automáticamente por el clúster.
Parado	En este estado, se evaluará el servicio para iniciar después de la transición del próximo servicio o nodo. Se trata de un estado temporal. Puede inhabilitar o habilitar el servicio desde este estado.
Fallido	El servicio se presume muerto. El servicio pasa a este estado cuando falla la operación de *parar* del recurso. Después de que pasa un servicio a este estado, debe verificar si no hay recursos asignados (sistemas de archivos montados, por ejemplo) antes de expedir una solicitud de **disable**. La única operación que puede llevarse a cabo cuando el servicio ha entrado en este estado es **disable**.
No inicializado	Este estado puede aparecer en algunos casos durante el inicio o ejecución de **clustat -f**.

Ejemplo 8.3. Pantalla clustat

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:15 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                  Owner (Last)                  State
 ------- ----                  ----- ------                  -----
 service:example_apache        node-01.example.com           started
 service:example_apache2       (none)                        disabled
```

8.3.2. Cómo administrar servicios de alta disponibilidad con clusvcadm

Puede manejar servicios de alta disponibilidad mediante el comando **clusvcadm**. Con él puede realizar las siguientes operaciones:

- Habilitar e iniciar el servicio.
- Inhabilitar un servicio.
- Parar un servicio.
- Congelar un servicio
- Descongelar un servicio

- Migrar un servicio (para servicios de máquina virtual únicamente)
- Reubicar un servicio.
- Reiniciar un servicio.

La Tabla 8.2, “Operaciones de servicio” describe las operaciones en más detalle. Para obtener una descripción completa de cómo realizar esas operaciones, consulte la herramienta de la página de manual **clusvcadm**.

Tabla 8.2. Operaciones de servicio

Operación de servicio	Descripción	Sintaxis de comandos

Operación de servicio	Descripción	Sintaxis de comandos

Operación de servicio	Descripción	Sintaxis de comandos

Operación de servicio	Descripción	Sintaxis de comandos
Activar	Inicia el servicio, opcionalmente en el destino preferido según las reglas de dominio de conmutación. En ausencia de un destino preferido o reglas de dominio de conmutación, el host local donde se ejecuta **clusvcadm** iniciará el servicio. Si el *Iniciar* falla, el servicio se comportará como si se hubiese solicitado una operación de *reubicar* (consulte **Reubicar** en esta tabla). Si la operación tiene éxito, el servicio se localizará en el estado iniciado.	**clusvcadm -e <service_name>** o **clusvcadm -e <service_name> -m <member>** (Mediante la opción -m especifica el miembro de destino preferido en el cual iniciar el servicio).
Inhabilitar	Detiene el servicio y lo pasa al estado inhabilitado. Esto solamente se permite cuando el servicio está en un estado *fallido*.	**clusvcadm -d <service_name>**
Reubicar	Desplaza el servicio a otro nodo. También puede especificar un nodo preferido para recibir el servicio, pero la incapacidad del servicio para que se ejecute en ese host (por ejemplo, si no se puede iniciar el servicio o si el host está desconectado) no impide la reubicación, y se elige otro nodo. **rgmanager** intenta iniciar el servicio en cada nodo del clúster admisible. Si ningún nodo de destino admisible en el clúster comienza con éxito el servicio, se produce un error en el traslado y el servicio intenta reiniciarse al propietario original. Si el propietario original no puede reiniciar el servicio, el servicio pasa al estado *Parado*	**clusvcadm -r <service_name>** o **clusvcadm -r <service_name> -m <member>** (El uso de la opción -m especifica el miembro de destino preferido en el cual iniciar el servicio).
Parar	Detiene el servicio y lo pasa al estado *Parado*.	**clusvcadm -s <service_name>**
Congelar	Congela el servicio en el nodo en que se esté ejecutando. Así evita que la verificación de estatus del servicio y la conmutación si el nodo falla o rgmanager se detiene. Se puede utilizar para suspender el servicio para permitir el mantenimiento de los recursos subyacentes. Consulte, "Consideraciones para el uso de las operaciones de congelar y descongelar" para obtener información importante sobre el uso de las operaciones *congelar* y *descongelar*.	**clusvcadm -Z <service_name>**
Descongelar	Saca un servicio del estado *congelar*. De esta manera, rehabilita las revisiones de estatus. Consulte "Consideraciones para el uso de las operaciones de congelar y descongelar" para obtener información importante sobre el uso de las operaciones *congelar* y *descongelar*.	**clusvcadm -U <service_name>**

Operación de servicio	Descripción	Sintaxis de comandos
Migrar	Migra una máquina virtual a otro nodo. Debe especificar un nodo de destino. Según la falla, si no puede migrar, la máquina virtual puede resultar en el estado *fallido* o en el estado iniciado en el propietario original.	`clusvcadm -M <service_name> -m <member>` **Importante** Para la operación de *migrar*, *debe especificar* un nodo de destino mediante la opción `-m <member>`.
Reiniciar	Reinicie el servicio en el nodo en el que se está ejecutando actualmente.	`clusvcadm -R <service_name>`

Consideraciones para el uso de las operaciones de congelar y descongelar

El uso de la operación *Congelar* permite el mantenimiento de partes de servicios `rgmanager`. Por ejemplo, si tiene una base de datos y un servidor de Web en un servicio `rgmanager`, puede congelar el servicio `rgmanager`, detener la base de datos, realizar mantenimiento, reiniciar la base de datos, y descongelar el servicio.

Cuando un servicio está congelado, se comporta así:

- Las verificaciones de *Estatus* se desactivan.
- Las operaciones de *Inicio* se desactivan.
- Las operaciones de *Parar* se inhabilitan.
- La conmutación no ocurrirá (incluso si apaga al propietario del servicio).

Importante

Si no sigue estos lineamientos puede hacer que los recursos se asignen a varios hosts:

- *No debe* parar todas las instancias de rgmanager cuando un servicio esté congelado a menos que planee reiniciar los hosts antes de reiniciar rgmanager.
- *No debe* descongelar un servicio hasta que el propietario reportado del servicio reconecte el clúster y reinicie el rgmanager.

8.4. Cómo actualizar una configuración

La actualización de configuración de clúster consiste en editar el archivo de configuración de clúster (`/etc/cluster/cluster.conf`) y propagarlo en cada nodo en el clúster. Puede actualizar la configuración mediante cualquiera de los siguientes procedimientos:

- Sección 8.4.1, “Cómo actualizar una configuración con `cman_tool version -r`”
- Sección 8.4.2, “Actualizar y configurar mediante `scp`”

8.4.1. Cómo actualizar una configuración con `cman_tool version -r`

Para actualizar la configuración mediante el comando `cman_tool version -r`, siga los siguientes pasos:

1. En cualquier nodo en el clúster, edite el archivo `/etc/cluster/cluster.conf`
2. Actualice el atributo `config_version` aumentando su valor (por ejemplo, cambiar de `config_version="2"` a `config_version="3">`).
3. Guarde `/etc/cluster/cluster.conf`.
4. Ejecute el comando `cman_tool version -r` para propagar la configuración para los nodos de clúster restantes. Es necesario que `ricci` esté ejecutándose en cada nodo de clúster para que pueda propagar la información de configuración de clúster.
5. Verifique si el archivo de configuración actualizado se ha propagado.

6. Puede obviar este paso (reiniciando el software de clúster) si ha hecho solamente los siguientes cambios de configuración:
   - Borrado de un nodo de una configuración de cluster—*excepto* cuando la cuenta de nodos cambia de mayor de dos nodos a dos nodos. Para obtener información sobre borrar un nodo de un clúster y pasarlo de mayor de dos nodos a dos nodos, consulte la Sección 8.2, “Borrar o añadir un nodo”.
   - Añadir un nodo a la configuración de cluster—*excepto* donde la cuenta de nodos cambia de dos nodos a más de dos nodos. Para obtener mayor información sobre la adición de un nodo a un clúster y la transición de dos nodos a más de dos nodos, consulte la Sección 8.2.2, “Adición de un nodo a un cluster”.
   - Cambios de cómo los demonios registran información.
   - Mantenimiento de Máquina virtual/servicio de alta disponiblidad (adición, edición o borrado).
   - Mantenimiento de recursos (adición, edición o borrado).
   - Mantenimiento de dominio de conmutación (adición, edición, o borrado).

   De lo contrario, debe reiniciar el software de clúster así:

   a. En cada nodo, pare el software de clúster de acuerdo con la Sección 8.1.2, “Cómo detener el software de clúster”. Por ejemplo:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

   b. En cada nodo, inicie el software de clúster de acuerdo con la Sección 8.1.1, “Cómo iniciar software de clúster”. Por ejemplo:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example"
now active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

   Parar e iniciar el software de clúster garantiza que los cambios de configuración que

han sido revisados solamente al inicio se incluyan en la configuración que está ejecutándose.

7. En cualquier nodo de clúster, ejecute **cman_tool nodes** para verificar los nodos que funcionan como miembros en el cluster (representado como "M" en la columna de estatus, "Sts"). Por ejemplo:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

8. En cualquier nodo, mediante la herramienta **clustat**, verifique si los servicios de alta disponibilidad se están ejecutando como esperado. Además, **clustat** muestra el estatus de los nodos de clúster. Por ejemplo:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    -----
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)                         disabled
```

9. Si el clúster está ejecutándose como se espera, ya ha terminado de actualizar la configuración.

8.4.2. Actualizar y configurar mediante scp

Para actualizar la configuración mediante el comando **scp**, siga los siguientes pasos:

1. En cada nodo, pare el software de clúster de acuerdo con la Sección 8.1.2, "Cómo detener el software de clúster". Por ejemplo:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

2. En cualquier nodo en el clúster, edite el archivo **/etc/cluster/cluster.conf**
3. Actualice el atributo **config_version** aumentando su valor (por ejemplo, cambiar de **config_version="2"** a **config_version="3">**).
4. Guarde **/etc/cluster/cluster.conf**.
5. Valide y actualice el archivo con el esquema de clúster (**cluster.rng**) al ejecutar el comando **ccs_config_validate**. Por ejemplo:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

6. Si el archivo actualizado es válido, use el comando **scp** para propagar a **/etc/cluster/** en cada nodo de clúster.
7. Verifique si el archivo de configuración actualizado se ha propagado.
8. En cada nodo, inicie el software de clúster de acuerdo con la Sección 8.1.1, “Cómo iniciar software de clúster”. Por ejemplo:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example" now
active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

9. En cualquier nodo de clúster, ejecute **cman_tool nodes** para verificar los nodos que funcionan como miembros en el cluster (representado como "M" en la columna de estatus, "Sts"). Por ejemplo:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

10. En cualquier nodo, mediante la herramienta **clustat**, verifique si los servicios de alta disponibilidad se están ejecutando como esperado. Además, **clustat** muestra el estatus de los nodos de clúster. Por ejemplo:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    -----
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)                         disabled
```

11. Si el clúster está ejecutándose como se espera, ya ha terminado de actualizar la configuración.

Capítulo 9. Cómo diagnosticar y corregir problemas en un clúster

9.1. Los cambios de configuración no se efectúan

9.2. El clúster no se forma

9.3. Nodos que no pueden reconectar clúster tras un cercado o reinicio

9.4. El demonio de clúster se bloquea
9.4.1. Captura del núcleo `rgmanager` en tiempo de ejecución
9.4.2. Captura del núcleo cuando el demonio se bloquea
9.4.3. Registro de una sesión `gdb` de seguimiento

9.5. Colgado de servicios de clúster

9.6. El servicio de clúster no iniciará

9.7. Servicio controlado de clúster falla al migrar

9.8. Cada nodo en un reporte de clúster de dos nodos reporta el segundo nodo caído

9.9. Nodos se cercan en Falla de ruta LUN

9.10. El disco de cuórum no aparece como miembro de clúster

9.11. Conducta de conmutación inusual

9.12. El cercado se presenta en forma aleatoria

9.13. El registro de depuración para el Gestor de bloqueo distribuido (DLM) necesita estar habilitado.

Los problemas de clúster, por naturaleza, pueden ser difíciles de solucionar. Esto se debe a la complejidad aumentada que un clúster de sistema introduce en contraposición con un sistema sencillo. Sin embargo, hay problemas comunes que los administradores de sistemas probablemente encontrarán al implementar o administrar un clúster. Entender cómo enfrentar esos problemas comunes puede ayudar a facilitar la implementación y administración de clúster.

Este capítulo proporciona información sobre algunos problemas comunes de clúster y cómo resolverlos. Puede encontrar ayuda adicional en su base de conocimientos y contactando al representante autorizado de soporte técnico de Red Hat. Si el problema se relaciona específicamente con el sistema de archivos GFS2, puede encontrar información sobre solución de problemas comunes de GFS2 en el documento *Sistema de archivos global2*.

9.1. Los cambios de configuración no se efectúan

Al hacer cambios a una configuración de clúster, debe propagar dichos cambios a cada nodo en el clúster.

- Al configurar un clúster mediante **Conga**, **Conga** propaga los cambios de forma automática cuando aplica los cambios.
- Para obtener información sobre cómo propagar cambios al clúster con el comando **ccs**, consulte la Sección 5.15, “Cómo propagar el archivo de configuración a los nodos de clúster”.
- Para obtener información sobre cómo propagar cambios al clúster con las herramientas de línea de comandos, consulte la Sección 8.4, “Cómo actualizar una configuración”.

Si hace alguno de los siguientes cambios de configuración al clúster, no se requiere reiniciar el clúster después de propagar dichos cambios para que los cambios se efectúen.

- Borrado de un nodo de una configuración de clúster—*excepto* cuando la cuenta de nodos cambia de mayor de dos nodos a dos nodos.
- Adición de un nodo a la configuración de clúster—*excepto* cuando el conteo de nodos cambie de dos nodos a mayor de dos.
- Cambio de parámetros de registro.
- Adición, edición o borrado de servicios de alta disponibilidad o componentes de máquina virtual (VM).
- Adición, edición o borrado de recursos de clúster.
- Adición, edición o borrado de dominios de conmutación.

No obstante, si hace otros cambios de configuración a su clúster, deberá reiniciar el clúster para

implementar dichos cambios. Los cambios a continuación requieren el reinicio de un clúster para que se efectúen:

- Adición o retiro de la opción **two_node** del archivo de configuración de clúster.
- Renombrar el clúster.
- Cambio de temporizadores **corosync** u **openais**.
- Heurística de adición, cambio o borrado para disco de cuórum , para cambiar cualquier temporizador de disco de cuórum o cualquier dispositivo de disco de cuórum. Para que dichos cambios se efectúen, se requerirá un reinicio global del **qdiskd**.
- Cambio del modo **central_processing** para **rgmanager**. Para que este cambio se efectúe se requiere un reinicio global de **rgmanager**.
- Cambio de dirección multidifusión.
- Cambio del modo de transporte de multidifusión UDP a unidifusión UDP o cambio de unidifusión UDP a multidifusión UDP.

Puede reiniciar el clúster mediante **Conga**, el comando **ccs** o la línea de comandos.

- Para obtener información sobre cómo reiniciar un clúster con **Conga**, consulte la Sección 4.4, “Iniciar, parar, reiniciar, y borrar clústeres”.
- Para obtener información sobre cómo reiniciar un clúster con el comando **ccs**, consulte la Sección 6.2, “Cómo iniciar y detener un clúster”.
- Para obtener información sobre cómo reiniciar un clúster con las herramientas de línea de comandos, consulte la Sección 8.1, “Iniciar y parar el software de clúster”.

9.2. El clúster no se forma

Si no puede hacer que se forme un clúster, revise lo siguiente:

- Asegúrese de establecer correctamente el nombre de resolución. El nombre de nodo de clúster en el archivo **cluster.conf** debe corresponder al nombre utilizado para resolver la dirección de cluster en la red que el clúster estará utilizando para comunicarse. Por ejemplo, si sus nombres de nodo de clúster son **nodea** y **nodeb** asegúrese de que ambos nodos tengan entradas en el archivo **/etc/cluster/cluster.conf** y **/etc/hosts** que coincidan con esos nombres.
- Puesto que el clúster usa multidifusión para la comunicación entre nodos, asegúrese de que el tráfico de multidifusión no esté bloqueado, retrasado o cruzado con la red que el clúster está utilizando para comunicarse. Observe que algunos interruptores de Cisco tienen funcionalidades que pueden causar retrasos en tráfico de multidifusión.
- Use **telnet** o **SSH** para verificar si puede conectar nodos remotos.
- Ejecute el comando **ethtool eth1 | grep link** para revisar si el enlace de Ethernet está activo.
- Use el comando **tcpdump** en cada nodo para revisar el tráfico de redes.
- Asegúrese de no tener reglas de cortafuegos bloqueando la comunicación entre sus nodos.
- Verifique si las interfaces que utiliza el clúster usan la comunicación internodos ahora utiliza el modo de enlace diferente a 0, 1, o 2. (los modos de enlace 0 y 2 tienen soporte a partir de Red Hat Enterprise Linux 6.4.)

9.3. Nodos que no pueden reconectar clúster tras un cercado o reinicio

Si sus nodos no se reconectan al clúster tras de un cercado o reinicio, revise lo siguiente:

- Los clústeres que están pasando su tráfico a través de un interruptor Cisco Catalyst pueden experimentar este problema.
- Asegúrese de que todos los nodos de clúster tengan la misma versión del archivo **cluster.conf**. Si el archivo **cluster.conf** es diferente a alguno de los nodos, entonces podrá conectar el clúster después de la valla.

  A partir del lanzamiento de Red Hat Enterprise 6.1, puede utilizar el siguiente comando para verificar que todos los nodos especificados en el archivo de configuración de clúster de host tengan el archivo de configuración de clúster idéntico:

  ```
  ccs -h host --checkconf
  ```

  Par obtener mayor información sobre el comando **ccs**, consulte Capítulo 5, *Configuración de adición de alta disponibilidad de Red Hat con el comando **ccs*** y Capítulo 6, *Administración de adición de alta disponibilidad de Red Hat con **ccs***.

- Asegúrese de haber configurado **chkconfig on** para servicios de clúster en el nodo que está intentando unirse al clúster.
- Asegúrese de que las reglas de cortafuegos no estén impidiendo que el nodo se comunique con otros nodos en el clúster.

9.4. El demonio de clúster se bloquea

RGManager tiene un proceso de vigilancia que reinicia el host si el proceso principal **rgmanager** falla de repente. Esto hace que el nodo de clúster se cerque y **rgmanager** recupere el servicio en otro host. Cuando el demonio detecta que el proceso principal **rgmanager** se ha bloqueado, entonces reiniciará el nodo de clúster y los nodos de clúster activos detectarán que el nodo de clúster ha salido y lo sacarán del clúster.

El *ID de proceso* con el número inferior (PID) es un proceso de vigilancia que se realiza si el hijo (el proceso con el número de PID más alto) se bloquea. Si captura el núcleo del proceso con el número de PID más alto mediante **gcore** puede ayudar durante la corrección de un demonio bloqueado.

Instale los paquetes requeridos para capturar y ver el núcleo y garantizar que tanto **rgmanager** como **rgmanager-debuginfo** tengan la misma versión o si no, el núcleo de la aplicación capturado puede ser inservible.

```
$ yum -y --enablerepo=rhel-debuginfo install gdb rgmanager-debuginfo
```

9.4.1. Captura del núcleo rgmanager en tiempo de ejecución

Hay dos procesos de **rgmanager** que están en ejecución cuando se inicia. Debe capturar el núcleo para el proceso **rgmanager** con el PID más alto.

A continuación verá un ejemplo de salida del comando **ps** que muestra dos procesos para **rgmanager**.

```
$ ps aux | grep rgmanager | grep -v grep

root     22482  0.0  0.5  23544  5136 ?        S<Ls Dec01   0:00 rgmanager
root     22483  0.0  0.2  78372  2060 ?        S<l  Dec01   0:47 rgmanager
```

En el siguiente ejemplo, el programa **pidof** sirve para determinar el número superior de PID, el cual es el PID apropiado para crear el núcleo. El comando completo captura el núcleo de la aplicación para el proceso 22483 que tiene el número más alto de PID.

```
$ gcore -o /tmp/rgmanager-$(date '+%F_%s').core $(pidof -s rgmanager)
```

9.4.2. Captura del núcleo cuando el demonio se bloquea

El script **/etc/init.d/functions** bloquea, de forma predeterminada, los archivos de núcleo desde los demonios llamados **/etc/init.d/rgmanager**. Para que el demonio cree núcleos de aplicaciones, debe habilitar esa opción. Este procedimiento debe realizarse en todos los nodos de clúster que necesitan una núcleo de aplicación capturado.

Para crear un archivo de núcleo cuando el demonio rgmanager se bloquee, modifique el archivo **/etc/sysconfig/cluster**. El parámetro ***DAEMONCOREFILELIMIT*** permite al núcleo del demonio la creación de archivos de núcleo si el proceso se bloquea. Existe una opción **-w** que evita la ejecución del proceso de vigilancia. El demonio de vigilancia. El demonio de vigilancia es responsable del reinicio del nodo del clúster si **rgmanager** se cuelga y algunos casos, si el demonio de vigilancia está ejecutándose entonces el archivo de núcleo no se generará, por lo tanto debe inhabilitarse para capturar archivos de núcleo.

```
DAEMONCOREFILELIMIT="unlimited"
RGMGR_OPTS="-w"
```

Reinicie rgmanager para activar las nuevas opciones de configuración:

```
service rgmanager restart
```

Nota

Si los servicios de clúster se están ejecutando en este nodo de clúster, entonces este podría abandonar los servicios en ejecución en un mal estado.

El archivo de núcleo se escribirá cuando se genere de un bloqueo del proceso **rgmanager**.

```
ls /core*
```

La salida debe ser similar a la siguiente:

```
/core.11926
```

Desplace o borre los archivos viejos de núcleo que están bajo el directorio / antes de reiniciar **rgmanager** para capturar el núcleo de aplicación. El nodo de clúster que experimentó el bloqueó de **rgmanager** debe reiniciarse o cercarse después de que el núcleo sea capturado para garantizar que el proceso de vigilancia no esté en ejecución.

9.4.3. Registro de una sesión gdb de seguimiento

Una vez que haya capturado el archivo de núcleo, puede ver su contenido mediante **gdb**, el depurador GNU. Para registrar una sesión de script del **gdb** en el archivo de núcleo desde el sistema afectado, ejecute lo siguiente:

```
$ script /tmp/gdb-rgmanager.txt
$ gdb /usr/sbin/rgmanager /tmp/rgmanager-.core.
```

Esto iniciará la sesión **gdb**, mientras que **script** lo registra en el archivo de texto apropiado. Cuando esté en **gdb**, ejecute los siguientes comandos:

```
(gdb) thread apply all bt full
(gdb) quit
```

Presione **ctrl-D** para detener la sesión de script y guárdela en el archivo de texto.

9.5. Colgado de servicios de clúster

Cuando los servicios de clúster intentan cercar un nodo, los servicios de clúster se detendrán hasta que la operación de cercado culmine con éxito. Por lo tanto, si el almacenaje controlado de clúster o servicios se cuelgan y los nodos de clúster muestran diferentes vistas de membresía de clúster o si el clúster se cuelga al tratar de cercar un nodo para reiniciar nodos a recuperar, revise las siguientes condiciones:

- El clúster puede haber intentado cercar un nodo y la operación de valla puede haber fallado.
- Observe en el archivo **/var/log/messages** en todos los nodos y vea si hay mensajes de vallas fallidos. Si los hay, reinicie los nodos en el clúster y configure correctamente el cercado.
- Verifique que la partición de red no ocurrió, como se describe en la Sección 9.8, “Cada nodo en un reporte de clúster de dos nodos reporta el segundo nodo caído”. También verifique si la comunicación entre nodos es aún posible y si la red está activa.
- Si nodos abandonan el clúster, habrá falta de cuórum. El clúster necesita tener cuórum de nodos para funcionar. Si se retiran nodos de tal forma que el clúster ya no tiene cuórum, los servicios y el almacenamiento se colgarán. Puede ajustar los votos esperados o retornar al clúster la cantidad de nodos requerida.

Nota

Puede cercar de forma manual un nodo con el comando **fence_node** o con **Conga**. Para obtener información, consulte la página de manual **fence_node** y la Sección 4.3.2, “Hacer que un nodo abandone o se una a un clúster”.

9.6. El servicio de clúster no iniciará

Si un servicio controlado de clúster no se inicia, revise las siguientes condiciones.

- Puede haber un error de sintaxis en el archivo **cluster.conf**. Use el comando **rg_test** para validar la sintaxis en su configuración. Si hay fallas de configuración o sintaxis, **rg_test** le dirá cual es el problema.

  ```
  $ rg_test test /etc/cluster/cluster.conf start service servicename
  ```

  Para obtener mayor información sobre el comando **rg_test**, consulte la Sección C.5,

"Depuración y prueba de servicios y ordenamiento de recursos".

Si la configuración es válida, entonces el registro del gestor de grupo de recursos aumenta y lee los registros de mensajes para determinar lo que está haciendo que el inicio del servicio falle. Puede aumentar el nivel de registro al adicionar el parámetro `loglevel="7"` a la etiqueta `rm` en el archivo `cluster.conf`. Luego obtendrá verbosidad en sus registros de mensajes respecto a iniciación, detención y migración de servicios en clúster.

9.7. Servicio controlado de clúster falla al migrar

Si un servicio controlado de clúster falla al migrar a otro nodo, pero el servicio se reinicia en un nodo específico, revise las siguientes condiciones.

- Asegúrese de que los recursos requeridos para ejecutar un servicio determinado estén presentes en todos los nodos en el clúster que pueden requerirse para ejecutar ese servicio. Por ejemplo, si su servicio de clúster asume que hay un archivo de script en una ubicación específica o un sistema de archivos montado en un punto de montaje específico, entonces debe asegurarse de que todos esos recursos estén disponibles en los lugares esperados en todos los nodos en el clúster.
- Asegúrese de que los dominios de conmutación, la dependencia del servicio y la exclusividad del servicio no estén configurados de tal forma que usted no pueda migrar servicios a nodos como lo esperaría.
- Si el servicio en cuestión es un recurso de máquina virtual, revise la documentación para asegurarse de que todo el trabajo de configuración ha sido completado.
- Aumente el registro de gestor de grupo de recursos, como se describe en la Sección 9.6, "El servicio de clúster no iniciará", y luego lea los registros de mensajes para determinar lo que está ocasionando que el inicio del servicio falle al migrar.

9.8. Cada nodo en un reporte de clúster de dos nodos reporta el segundo nodo caído

Si su clúster es de dos nodos y cada nodo reporta que está activo pero que hay un nodo inactivo, significa que sus nodos de clúster no pueden comunicarse con otro vía multidifusión en la red de latidos de clúster. Este problema se conoce como "cerebro dividido" o una "partición de red." Para solucionarlo, revise las condiciones descritas en la Sección 9.2, "El clúster no se forma".

9.9. Nodos se cercan en Falla de ruta LUN

Si un nodo o nodos en su clúster se cerca cada vez que tiene una falla de ruta LUN, puede ser el resultado del uso de un disco de cuórum en el almacenamiento de multirutas. Si está utilizando un disco de cuórum y su disco de cuórum está en almacenamiento de multirutas, asegúrese de tener configurados correctamente todos los tiempos para tolerar una falla de rutas.

9.10. El disco de cuórum no aparece como miembro de clúster

Si ha configurado su sistema para usar un disco de cuórum, pero el disco de cuórum no aparece como miembro de su clúster, revise las siguientes condiciones:

- Asegúrese de tener `chkconfig on` para el servicio `qdisk`.
- Asegúrese de haber iniciado el servicio `qdisk`.
- Observe que puede tomar varios minutos para que el disco de cuórum se registre al clúster. Esta es una conducta normal y esperada.

9.11. Conducta de conmutación inusual

Un problema común con los servidores de clúster es la conducta de conmutación inusual. Los servicios se detendrán cuando otros servicios inician o los servicios rehusarán iniciar en conmutación. Esto puede deberse a tener sistemas de conmutación complejos que constan de dominios de conmutación, dependencia de servicios y exclusividad de servicios. Intente un servicio o configuración de dominio de conmutación más sencillo y observe si el problema persiste. Evite funcionalidades de exclusividad de servicios y dependencia, a menos que entienda totalmente cómo pueden afectar la conmutación en todas las circunstancias.

9.12. El cercado se presenta en forma aleatoria

Si encuentra que un nodo se cerca de forma aleatoria, revise las siguientes condiciones:

- La causa de las vallas es *siempre* un nodo que pierde el símbolo, es decir que pierde la comunicación con el resto del clúster y se detiene retornando latidos.

- Cualquier situación que resulte en un sistema que no retorne latidos dentro de un intervalo de símbolo especificado puede conducir a una valla. El intervalo de símbolo predeterminado es de 10 segundos. Puede ser especificado al añadir el valor deseado (en ms) al parámetro de símbolo de la etiqueta de totem en el archivo **cluster.conf** (por ejemplo, si establece un **totem token="30000"** para 30 segundos).
- Verifique si la red es segura y está funcionando como se espera.
- Verifique si las interfaces que utiliza el clúster usan la comunicación internodos ahora utiliza el modo de enlace diferente a 0, 1, o 2. (los modos de enlace 0 y 2 tienen soporte a partir de Red Hat Enterprise Linux 6.4.)
- Tome medidas para determinar si el sistema se está "congelando" o si hay una emergencia de kernel. Configure la herramienta **kdump** y observe si obtiene un núcleo en una de esas vallas.
- Asegúrese que no se esté presentando alguna situación en la que usted esté erróneamente atribuyendo al cercado, por ejemplo el disco de cuórum que expulsa un nodo debido a una falla o a un producto de terceros tales como reinicio de RAC Oracle debido a alguna condición externa. Los registros de mensajes siempre son muy útiles para determinar dichos problemas. Cuando se presentan reinicios de vallas o nodos debería ser una práctica común inspeccionar los registros de mensajes de todos los nodos en el clúster desde que se presentan el reinicio y el cercado.
- Revise detenidamente el sistema por si hay fallas de hardware que puedan hacer que el sistema no responda a los latidos cuando se espera.

9.13. El registro de depuración para el Gestor de bloqueo distribuido (DLM) necesita estar habilitado.

Hay dos opciones de depuración para el Gestor de bloqueo distribuido (DLM) que usted puede habilitar, si es necesario: la depuración de kernel DLM y la depuración de bloqueo POSIX.

Para habilitar la depuración DLM, edite el archivo **/etc/cluster/cluster.conf** para añadir opciones de configuración a la etiqueta **dlm**. La opción **log_debug** habilita los mensajes de depuración de kernel DLM y la opción **plock_debug** habilita los mensajes de depuración de bloqueo POSIX.

La siguiente sección de ejemplo de un archivo **/etc/cluster/cluster.conf** muestra la etiqueta de **dlm** que activa ambas opciones de depuración DLM:

```
<cluster config_version="42" name="cluster1">
  ...
  <dlm log_debug="1" plock_debug="1"/>
  ...
</cluster>
```

Después de editar el archivo **/etc/cluster/cluster.conf**, ejecute el comando **cman_tool version -r** para propagar la configuración al resto de los nodos de clúster.

Capítulo 10. Configuración de SNMP con adición de alta disponibilidad de Red Hat

10.1. SNMP y adición de alta disponibilidad de Red Hat

10.2. Configuración SNMP con la adición de alta disponibilidad de Red Hat

10.3. Cómo reenviar capturas SNMP

10.4. Capturas SNMP producidas por la adición de alta disponibilidad de Red Hat

A partir del lanzamiento de Red Hat Enterprise Linux 6.1, la adición de alta disponibilidad de Red Hat proporciona soporte para capturas SNMP. Este capítulo describe cómo configurar su sistema para SNMP seguido de un resumen de capturas emitidas por la adición de alta disponibilidad de Red Hat para eventos de clúster.

10.1. SNMP y adición de alta disponibilidad de Red Hat

El subagente SNMP de adición de alta disponibilidad de Red Hat es **foghorn**, el cual emite las capturas SNMP. El subagente **foghorn** se comunica con el demonio **snmpd** mediante el protocolo AgentX. El subagente **foghorn** solamente crea capturas SNMP; no soporta otras funciones de SNMP tales como **get** o **set**.

No hay opciones **config** para el subagente **foghorn**. No puede ser configurado para usar un socket específico; solamente el socket AgentX predeterminado es compatible en el momento.

10.2. Configuración SNMP con la adición de alta disponibilidad de Red Hat

Para configurar SNMP con la adición de alta disponibilidad de Red Hat, realice los siguientes pasos en cada nodo en el clúster para asegurarse de que los servicios necesarios estén activados y en ejecución.

1. Para usar capturas SNMP con adiciones de alta disponibilidad de Red Hat, el servicio **snmpd** es requerido y actúa como el agente maestro. Puesto que el servicio **foghorn** es el subagente y utiliza el protocolo AgentX, debe añadir la siguiente línea al archivo **/etc/snmp/snmpd.conf** para activar el soporte de AgentX:

   ```
   master agentx
   ```

2. Para especificar a dónde se deben enviar las notificaciones de capturas SNMP, añada la siguiente línea al archivo **/etc/snmp/snmpd.conf**:

   ```
   trap2sink host
   ```

   Para obtener mayor información sobre manejo de notificaciones, consulte la página de manual **snmpd.conf**.

3. Asegúrese de que el demonio **snmpd** esté activado y en ejecución mediante los siguientes comandos:

   ```
   # chkconfig snmpd on
   # service snmpd start
   ```

4. Si el demonio **messagebus** no está activado aún y en ejecución, ejecute los siguientes comandos:

   ```
   # chkconfig messagebus on
   # service messagebus start
   ```

5. Asegúrese de que el demonio **foghorn** esté activo y en ejecución mediante los siguientes comandos:

   ```
   # chkconfig foghorn on
   # service foghorn start
   ```

6. Ejecute el siguiente comando para configurar su sistema con el fin de que **COROSYNC-MIB** genere capturas SNMP para garantizar que el demonio **corosync-notifyd** esté activo y en ejecución:

   ```
   $ echo "OPTIONS=\"-d\" " > /etc/sysconfig/corosync-notifyd
   $ chkconfig corosync-notifyd on
   $ service corosync-notifyd start
   ```

Tras haber configurado cada nodo en el clúster para SNMP y verificado que los servicios necesarios estén ejecutándose, se recibirán señales de D-bus mediante el servicio **foghorn** y traducidas a capturas SNMPv2. Dichas capturas luego se pasan al hosta que usted definió con la entrada **trapsink** para recibir capturas SNMPv2.

10.3. Cómo reenviar capturas SNMP

Es posible reenviar capturas SNMP a una máquina que no es parte del clúster donde usted puede usar el demonio **snmptrapd** en la máquina externa y personalizar cómo responder a esas notificaciones.

Realice los siguientes pasos para reenviar capturas SNMP en un clúster a una máquina que no es uno de los nodos de clúster:

1. Para cada nodo en el clúster, siga el procedimiento descrito en la Sección 10.2, "Configuración SNMP con la adición de alta disponibilidad de Red Hat", estableciendo la entrada **trap2sink *host*** en el archivo **/etc/snmp/snmpd.conf** para especificar el host externo que estará ejecutando el demonio **snmptrapd**.
2. En el host externo que recibirá las capturas, edite el archivo de configuración **/etc/snmp/snmptrapd.conf** para especificar sus cadenas comunitarias. Por ejemplo, puede usar la siguiente entrada para permitir que el demonio **snmptrapd** procese las notificaciones mediante la cadena comunitaria **public**.

   ```
   authCommunity log,execute,net public
   ```

3. En el host externo que recibirá las capturas, asegúrese de que el demonio **snmptrapd** esté activado y en ejecución mediante los siguientes comandos.

   ```
   # chkconfig snmptrapd on
   # service snmptrapd start
   ```

Para mayor información sobre el procesamiento de notificacione SNMP, consulte la página de manual **snmptrapd.conf**.

10.4. Capturas SNMP producidas por la adición de alta disponibilidad de Red Hat

El demonio **foghorn** genera las siguientes capturas:

- **fenceNotifyFenceNode**

  Esta captura se presenta cuando un nodo cercado intenta cercar otro nodo. Observe que esta captura solamente se genera en un nodo -- el nodo que intentó realizar esta operación de valla. La notificación incluye los siguientes campos:

  - **fenceNodeName** - nombre del nodo cercado
  - **fenceNodeID** - ID de nodo del nodo cercado
  - **fenceResult** - el resultado de la operación de valla (0 para correcto, -1 para cuando algo salió mal, -2 para métodos de cercado no definidos)

- **rgmanagerServiceStateChange**

  Esta captura se presenta cuando el estado de un servicio de clúster cambia. La notificación incluye los siguientes campos:

  - **rgmanagerServiceName** - el nombre del servicio, el cual incluye el tipo de servicio (por ejemplo, **service:foo** o **vm:foo**).
  - **rgmanagerServiceState** - el estado del servicio. Excluye los estados tales como **starting** y **stopping** para reducir bloqueos en las capturas.
  - **rgmanagerServiceFlags** - los indicadores del servicio. Actualmente hay dos indicadores con soporte: **frozen**, el cual indica un servicio que ha sido congelado mediante **clusvcadm -Z**, y **partial**, indicando un servicio en el cual un recurso fallido ha sido marcado como **non-critical** para que el recurso falle y sus componentes reinicien en forma manual sin que todo el servicio se afecte.
  - **rgmanagerServiceCurrentOwner** - el propietario del servicio. Si el servicio no está en ejecución, será **(none)**.
  - **rgmanagerServicePreviousOwner** - el último propietario del servicio conocido, si se conoce. Si el último propietario es desconocido, puede indicar **(none)**.

El demonio **corosync-nodifyd** genera las siguientes capturas:

- **corosyncNoticesNodeStatus**

  Esta captura se presenta cuando un nodo se conecta o abandona el clúster. La notificación incluye los siguientes campos:

  - **corosyncObjectsNodeName** - nombre de nodo
  - **corosyncObjectsNodeID** - ID de nodo
  - **corosyncObjectsNodeAddress** - dirección IP de nodo
  - **corosyncObjectsNodeStatus** - estatus de nodo (**joined** o **left**)

- **corosyncNoticesQuorumStatus**

  Esta captura se presenta cuando el estado de cuórum cambia. La notificación incluye los siguientes campos:

  - **corosyncObjectsNodeName** - nombre de nodo
  - **corosyncObjectsNodeID** - ID de nodo
  - **corosyncObjectsQuorumStatus** - nuevo estado del cuórum (**quorate** o **NOT quorate**)

- **corosyncNoticesAppStatus**

  Esta captura se presenta cuando la aplicación de clientes se conecta o desconecta de Corosync.

  - **corosyncObjectsNodeName** - nombre de nodo
  - **corosyncObjectsNodeID** - ID de nodo
  - **corosyncObjectsAppName** - nombre de aplicación
  - **corosyncObjectsAppStatus** - nuevo estado de aplicación (**connected** o **disconnected**)

Capítulo 11. Configuraciones de Samba en clúster

11.1. Visión general de CTDB

11.2. Paquetes requeridos

11.3. Configuración de GFS2

11.4. Configuración de CTDB

11.5. Configuración de Samba

11.6. Cómo iniciar CTDB y los servicios de Samba

11.7. Cómo usar el servidor Samba en clúster

A partir del lanzamiento de Red Hat Enterprise Linux 6.2, la adición de Alta disponibilidad de Red Hat ofrece soporte para Samba en clúster en una configuración activa/activa. Para esto se requiere que usted instale y configure CTDB en todos los nodos en un clúster que usted utiliza junto con sistemas de archivos GFS2 agrupados.

Nota

Red Hat Enterprise Linux 6 soporta un máximo de cuatro nodos ejecutando Samba en clúster.

Este capítulo describe el procedimiento para configurar CTDB mediante la configuración de un ejemplo. Para obtener información sobre cómo configurar los sistemas de archivos GFS2, consulte *Sistema de archivos global 2*. Para obtener información sobre cómo configurar volúmenes lógicos, consulte *Administración del gestor de volumen lógicos*.

11.1. Visión general de CTDB

CTDB es una implementación de la base de datos TDB utilizada por Samba. Para usar CTDB, debe estar disponible un sistema de archivos en clúster y compartirse en todos los nodos en el clúster. CTDB proporciona funcionalidades en clúster por encima de este sistema de archivos en clúster. A partir del lanzamiento 6.2 de Red Hat Enterprise Linux 6.2, CTDB también se ejecuta en una pila de clúster en paralelo con el provisto por el agrupamiento de Red Hat Enterprise Linux. CTDB administra membresía de nodos, recuperación/conmutación, reubicación de IP y servicios de Samba.

11.2. Paquetes requeridos

Aparte de los paquetes estándar que se requieren para ejecutar la adición de alta disponibilidad de Red Hat y la adición de almacenaje resistente de Red Hat, para ejecutar Samba con agrupamiento de Red Hat Enterprise Linux se requieren los siguientes paquetes:

- **`ctdb`**
- **`samba`**
- **`samba-common`**
- **`samba-winbind-clients`**

11.3. Configuración de GFS2

Para configurar Samba con agrupamiento de Red Hat Enterprise Linux se requieren dos sistemas de archivos GFS2: Un sistema de archivos pequeño para CTDB, y un segundo sistema de archivos para el recurso compartido de Samba. Este ejemplo muestra cómo crear los dos sistemas de archivos GFS2.

Antes de crear los sistemas de archivos GFS2, cree un volumen lógico LVM para cada uno de los sistemas de archivos. Para obtener información sobre cómo crear volúmenes lógicos LVM, consulte *Administración del gestor de volumen lógicos*. Este ejemplo usa los siguientes volúmenes lógicos:

- **`/dev/csmb_vg/csmb_lv`**, el cual guarda los datos de usuario que serán exportados a través de un recurso compartido de Samba y debe ajustarse al tamaño correspondiente. Este ejemplo crea un volumen lógico que tiene un tamaño de 100 GB.
- **`/dev/csmb_vg/ctdb_lv`**, el cual almacenará la información del estado de CTDB y necesita un tamaño de 1 GB.

Ha creado grupos de volumen en clúster y los volúmenes lógicos en un nodo del clúster

únicamente.

Para crear un sistema de archivos GFS2 en un volumen lógico, ejecute el comando **mkfs.gfs2**. Puede ejecutar este comando en un nodo de clúster únicamente.

Para crear un sistema de archivos para albergar el recurso compartido de Samba en un volumen lógico **/dev/csmb_vg/csmb_lv**, ejecute el siguiente comando:

```
[root@clusmb-01 ~]# mkfs.gfs2 -j3 -p lock_dlm -t csmb:gfs2 /dev/csmb_vg/csmb_lv
```

El significado de los parámetros es el siguiente:

-j
Especifica el número de diarios para crear en el sistema de archivos. Este ejemplo usa un clúster con tres nodos, por lo tanto creamos un diario por nodo.

-p
Especifica el protocolo de cerrojo. **lock_dlm** es el protocolo de cerrojo que GFS2 usa para comunicación entre nodos.

-t
Especifica el nombre de tabla de cerrojo y tiene el formato ***nombre de clúster:nombre de sistema de archivos***. En este ejemplo, el nombre del clúster como se especifica en el archivo **cluster.conf** es el **csmb**, y utilizamos **gfs2** como el nombre para el sistema de archivos.

La salida de este comando aparece así:

```
This will destroy any data on /dev/csmb_vg/csmb_lv.
  It appears to contain a gfs2 filesystem.

Are you sure you want to proceed? [y/n] y

Device:
/dev/csmb_vg/csmb_lv
Blocksize:              4096
Device Size             100.00 GB (26214400 blocks)
Filesystem Size:        100.00 GB (26214398 blocks)
Journals:               3
Resource Groups:        400
Locking Protocol:       "lock_dlm"
Lock Table:             "csmb:gfs2"
UUID:
  94297529-ABG3-7285-4B19-182F4F2DF2D7
```

En este ejemplo, el sistema de archivos **/dev/csmb_vg/csmb_lv** se montará en **/mnt/gfs2** sobre todos los nodos. Este punto de montaje debe coincidir con el valor que especifique como el sitio del directorio **share** con la opción **path =** en el archivo **/etc/samba/smb.conf**, como se describe en la Sección 11.5, “Configuración de Samba”.

Para crear el sistema de archivos que albergue la información de estado de CTBD en el volumen lógico **/dev/csmb_vg/ctdb_lv**, ejecute el siguiente comando:

```
[root@clusmb-01 ~]# mkfs.gfs2 -j3 -p lock_dlm -t
csmb:ctdb_state /dev/csmb_vg/ctdb_lv
```

Observe que este comando especifica un nombre de tabla de cerrojo diferente al de la tabla de cerrojo en el ejemplo que creó el sistema de archivos en **/dev/csmb_vg/csmb_lv**. Este distingue los nombres de tablas de cerrojo para los diferentes dispositivos utilizados para los sistemas de archivos.

La salida de **mkfs.gfs2** es la siguiente:

```
This will destroy any data on /dev/csmb_vg/ctdb_lv.
  It appears to contain a gfs2 filesystem.

Are you sure you want to proceed? [y/n] y

Device:
/dev/csmb_vg/ctdb_lv
Blocksize:              4096
Device Size             1.00 GB (262144 blocks)
Filesystem Size:        1.00 GB (262142 blocks)
Journals:               3
Resource Groups:        4
Locking Protocol:       "lock_dlm"
Lock Table:             "csmb:ctdb_state"
UUID:
  BCDA8025-CAF3-85BB-B062-CC0AB8849A03
```

En este ejemplo, el sistema de archivos **/dev/csmb_vg/ctdb_lv** se montará en **/mnt/ctdb** sobre todos los nodos. Este punto de montaje coincide con el valor que especifique como sitio para el archivo **.ctdb.lock** con la opción **CTDB_RECOVERY_LOCK** en el archivo **/etc/sysconfig/ctdb**, como se describe en la Sección 11.4, “Configuración de CTDB”.

11.4. Configuración de CTDB

El archivo de configuración CTDB se localiza en **/etc/sysconfig/ctdb**. Los campos obligatorios que deben configurarse para la operación de CTBD es la siguiente:

- **CTDB_NODES**
- **CTDB_PUBLIC_ADDRESSES**
- **CTDB_RECOVERY_LOCK**
- **CTDB_MANAGES_SAMBA** (debe estar activado)
- **CTDB_MANAGES_WINBIND** (debe estar activado si se ejecuta en un servidor miembro)

El siguiente ejemplo muestra los campos obligatorios de un archivo de configuración para que la operación CTDB se establezca con parámetros de ejemplo:

```
CTDB_NODES=/etc/ctdb/nodes
CTDB_PUBLIC_ADDRESSES=/etc/ctdb/public_addresses
CTDB_RECOVERY_LOCK="/mnt/ctdb/.ctdb.lock"
CTDB_MANAGES_SAMBA=yes
CTDB_MANAGES_WINBIND=yes
```

El significado de estos parámetros es el siguiente:

CTDB_NODES

Especifica la ubicación del archivo que contiene la lista de nodos de clúster.

El archivo **/etc/ctdb/nodes** que hace referencia a **CTDB_NODES** simplemente enumera las direcciones IP de los nodos de clúster, así como en el siguiente ejemplo:

```
192.168.1.151
192.168.1.152
192.168.1.153
```

En este ejemplo, hay únicamente una interfaz/IP en cada nodo que se utiliza para comunicación de clúster y CTDB y los clientes servidores. Sin embargo , se recomienda que cada nodo de usuario tenga dos interfaces de red para que una serie de interfaces pueda dedicarse al acceso de cliente público. Use las direcciones IP apropiadas de red de clúster aquí y asegúrese de que los nombres de host y direcciones IP utilizadas en el archivo **cluster.conf** sean las mismas. Igualmente, use las interfaces apropiadas de la red pública para acceder al cliente en el archivo **public_addresses**.

Es crucial que el archivo **/etc/ctdb/nodes** sea idéntico en todos los nodos porque el ordenamiento es importante y CTDB fallará si encuentra información diferente en nodos diferentes.

CTDB_PUBLIC_ADDRESSES

Especifica el sitio del archivo que lista las direcciones IP que pueden servir para acceder a los recursos compartidos de Samba exportados por este clúster. Se trata de direcciones IP que debe configurar en DNS para el nombre del servidor de Samba en clúster y de las direcciones a las que los clientes CIFS se conectarán. Configure el nombre del servidor de Samba en clúster como un registro de DNS tipo A con múltiples direcciones IP y permita que DNS round-robin distribuya los clientes a través de los nodos del clúster.

Para este ejemplo, hemos configurado una entrada DNS round-robin **csmb-server** con todas las direcciones listadas en el archivo **/etc/ctdb/public_addresses**. DNS distribuirá los clientes que usan dicha entrada a través del clúster a la manera de round-robin.

El contenido del archivo **/etc/ctdb/public_addresses** en cada nodo es el siguiente:

```
192.168.1.201/0 eth0
192.168.1.202/0 eth0
192.168.1.203/0 eth0
```

Este ejemplo muestra tres direcciones que actualmente no se utilizan en la red. En su propia configuración, elija las direcciones que pueden acceder los presuntos clientes.

Como otra alternativa, este ejemplo muestra el contenido de los archivos **/etc/ctdb/public_addresses** en un clúster en el cual hay tres nodos, pero un total de cuatro direcciones públicas. En este ejemplo, la dirección IP 198.162.2.1 puede ser el nodo 0 o el nodo 1 y estará disponible para clientes siempre y cuando al menos uno de estos nodos esté disponible. Solo si ambos nodos 0 y 1 fallan, la dirección pública no estará disponible para clientes. Las demás direcciones públicas solo pueden ser servidas por un nodo individual respectivamente y, por lo tanto, solo estarán disponibles si el respectivo nodo lo está.

El archivo **/etc/ctdb/public_addresses** en nodo 0 incluye el siguiente contenido:

```
198.162.1.1/24 eth0
198.162.2.1/24 eth1
```

El archivo **/etc/ctdb/public_addresses** en el nodo 1 incluye el siguiente contenido:

```
198.162.2.1/24 eth1
198.162.3.1/24 eth2
```

El archivo **/etc/ctdb/public_addresses** en el nodo 2 incluye el siguiente contenido:

```
198.162.3.2/24 eth2
```

CTDB_RECOVERY_LOCK

Especifica un archivo de cerrojo que CTDB usa internamente para recuperación. Este archivo debe residir en almacenaje compartido de tal forma que todos los nodos de clúster tengan acceso a él. El ejemplo en esta sección usa el sistema de archivos GFS2 que se montará en **/mnt/ctdb** en todos los nodos. Es diferente al sistema de archivos GFS2, el cual albergará al recurso compartido de Samba que será exportado. Este archivo de cerrojo de recuperación sirve para evitar escenarios de cerebro divido. Con versiones más recientes de CTDB (1.0.112 y posteriores), la especificación de este archivo es opcional siempre y cuando se sustituya por otro mecanismo de prevención de cerebro dividido.

CTDB_MANAGES_SAMBA

Al activar con **yes**, especifica que CTDB puede iniciar y detener el servicio de Samba, ya que se hace necesario proveer el servicio de migración y conmutación.

Cuando **CTDB_MANAGES_SAMBA** está activada, debe desactivar el inicio automático **init**, de los demonios **smb** y **nmb** con los siguientes comandos:

```
[root@clusmb-01 ~]# chkconfig snb off
[root@clusmb-01 ~]# chkconfig nmb off
```

CTDB_MANAGES_WINBIND

SI lo habilita con **yes**, especifica que la CTDB puede iniciar o parar el demonio **winbind** como se requiere. Debe estar activa cuando utilice CTDB en un dominio de Windows o en un modo de seguridad de directorio activo.

Cuando se habilita **CTDB_MANAGES_WINBIND**, deberá desactivar el inicio automático **init** del demonio **winbind** con el siguiente comando:

```
[root@clusmb-01 ~]# chkconfig windinbd off
```

11.5. Configuración de Samba

El archivo de configuración de Samba **smb.conf** se localiza en **/etc/samba/smb.conf** en este ejemplo. Contiene los siguientes parámetros::

```
[global]
        guest ok = yes
        clustering = yes
        netbios name = csmb-server
[csmb]
        comment = Clustered Samba
        public = yes
        path = /mnt/gfs2/share
        writeable = yes
        ea support = yes
```

Este ejemplo exporta un recurso compartido con el nombre **csmb** localizado en **/mnt/gfs2/share**. Este difiere del sistema de archivos compartido GFS2 en **/mnt/ctdb/.ctdb.lock** que especificamos como el parámetro **CTDB_RECOVERY_LOCK** en el archivo de configuracióon CTDB en **/etc/sysconfig/ctdb**.

En este ejemplo, crearemos el directorio **share** en **/mnt/gfs2** al montarlo por primera vez. La entrada **clustering = yes** le dice a Samba que utilice CTDB. La entrada **netbios name = csmb-server** establece de forma explícita todos los nodos para que tengan un nombre NetBIOS común. El parámetro **ea support** se requiere si planea usar atributos extendidos.

El archivo de configuración **smb.conf** debe ser idéntico en todos los nodos del clúster.

Samba también ofrece una configuración basada en registro mediante el comando **net conf** para mantener sincronizada la configuración de forma automática entre los miembros de clúster sin necesidad de copiar manualmente los archivos de configuración entre los nodos de clúster. Para obtener información sobre el comando **net conf**, consulte la página de manual **net**(8).

11.6. Cómo iniciar CTDB y los servicios de Samba

Después de iniciar el clúster, debe montar los sistemas de archivos GFS2 que ha creado, como se describe en la Sección 11.3, “Configuración de GFS2”. Los permisos en el directorio de Samba **share** y las cuentas de usuario en los nodos de clúster deben configurarse para acceso de cliente.

Ejecute el siguiente comando en todos los nodos para arrancar el demonio **ctdbd**. Ya que este ejemplo configuró CTDB con **CTDB_MANAGES_SAMBA=yes**, CTDB también iniciará el servicio Samba en todos los nodos y exportará todos los recursos compartidos de Samba configurados.

```
[root@clusmb-01 ~]# service ctdb start
```

También puede tomarse un par de minutos para que CTDB inicie Samba, exporte los recursos compartidos, y se estabilice. La ejecución de **ctdb status** muestra el estatus de CTDB, como en el siguiente ejemplo:

```
[root@clusmb-01 ~]# ctdb status
Number of nodes:3
pnn:0 192.168.1.151     OK (THIS NODE)
pnn:1 192.168.1.152     OK
pnn:2 192.168.1.153     OK
Generation:1410259202
Size:3
hash:0 lmaster:0
hash:1 lmaster:1
hash:2 lmaster:2
Recovery mode:NORMAL (0)
Recovery master:0
```

Cuando vea que todos los nodos están "OK", es seguro pasar a utilizar el servidor de Samba en clúster, como se describe en la Sección 11.7, “Cómo usar el servidor Samba en clúster”.

11.7. Cómo usar el servidor Samba en clúster

Los clientes se pueden conectar al recurso compartido de Samba que fue exportado al conectarse a una de las direcciones IP especificadas en el archivo **/etc/ctdb/public_addresses** o mediante la entrada de DNS **csmb-server** que configuramos antes, como se muestra a continuación:

```
[root@clusmb-01 ~]# mount -t cifs //csmb-server/csmb /mnt/sambashare -o
user=testmonkey
```

o

```
[user@clusmb-01 ~]$ smbclient //csmb-server/csmb
```

Parámetros de dispositivos de valla

Este apéndice proporciona tablas con descripciones de parámetros de recursos de dispositivos de valla de alta disponibilidad. Configure los parámetros con **luci**, mediante el comando `ccs` o al editar el archivo `etc/cluster/cluster.conf`. Para obtener una lista y una descripción completa de los parámetros de valla para cada agente de valla, consulte la página de manual para dicho agente.

Nota

El parámetro de **Nombre** para dispositivos de valla, especifica un nombre arbitrario para el dispositivo que será utilizado por la adición de alta disponibilidad de Red Hat. No es lo mismo que el nombre de DNS para el dispositivo.

Nota

Algunos dispositivos de valla tienen un parámetro de **Script de contraseña**. El parámetro de **Script de contraseña** le permite especificar que una contraseña de dispositivo de valla se suministre desde un script en lugar de hacerlo desde el parámetro de **Contraseña**. El uso del parámetro de **Script de contraseña** remplaza al parámetro de **Contraseña**, lo que permite que las contraseñas no sean visibles en el archivo de configuración de clúster (`/etc/cluster/cluster.conf`).

La Tabla A.1, “Resumen de dispositivos de valla” lista los dispositivos de valla, los agentes de dispositivos de valla asociados con los dispositivos de valla, y provee una referencia para la tabla que documenta los parámetros para los dispositivos de valla.

Tabla A.1. Resumen de dispositivos de valla

Dispositivo de valla	Agente de vallas	Referencia para descripción de parámetros

Dispositivo de valla	Agente de vallas	Referencia para descripción de parámetros
Dispositivo de valla	Agente de vallas	Referencia para descripción de parámetros

Dispositivo de valla	Agente de vallas	Referencia para descripción de parámetros
Interruptor APC (telnet/SSH)	fence_apc	Tabla A.2, “Interruptor APC (telnet/SSH)”
Interruptor Brocade Fabric	fence_brocade	Tabla A.4, “Interruptor Brocade Fabric”
Cisco MDS	fence_cisco_mds	Tabla A.5, “Cisco MDS”
Cisco UCS	fence_cisco_ucs	Tabla A.6, “Cisco UCS”
Dell DRAC 5	fence_drac5	Tabla A.7, “Dell DRAC 5”
Interruptor de energía de red Eaton (Interfaz SNMP).	fence_eaton_snmp	Tabla A.8, “El controlador de energía de red Eaton (Controlador SNMP) (Red Hat Enterprise Linux 6.4 y posteriores)”
Controlador Egenera SAN	fence_egenera	Tabla A.9, “Controlador Egenera SAN”
ePowerSwitch	fence_eps	Tabla A.10, “ePowerSwitch”
Fence virt	fence_virt	Tabla A.11, “Fence virt”
Fujitsu Siemens Remoteview Service Board (RSB)	fence_rsb	Tabla A.12, “Fujitsu Siemens Remoteview Service Board (RSB)”
HP BladeSystem	fence_hpblade	Tabla A.13, “HP BladeSystem (Red Hat Enterprise Linux 6.4 y posterior)”
HP iLO/iLO2 (Integrated Lights Out)	fence_ilo	Tabla A.14, “HP iLO/iLO2 (Integrated Lights Out)”
HP iLO (Integrated Lights Out) MP	fence_ilo_mp	Tabla A.15, “HP iLO (Integrated Lights Out) MP”
IBM BladeCenter	fence_bladecenter	Tabla A.16, “IBM BladeCenter”
IBM BladeCenter SNMP	fence_ibmblade	Tabla A.17, “IBM BladeCenter SNMP”
IBM iPDU	fence_ipdu	Tabla A.18, “IBM iPDU (Red Hat Enterprise Linux 6.4 y posterior)”
IF MIB	fence_ifmib	Tabla A.19, “IF MIB”
Intel Modular	fence_intelmodular	Tabla A.20, “Intel Modular”
	fence_ipmilan	Tabla A.21, “LAN IPMI (Interfaz de administración de plataforma inteligente)”

Dispositivo de valla	Agente de vallas	Referencia para descripción de parámetros
LAN IPMI (Interfaz de administración de plataforma inteligente)		
RHEV-M REST API	fence_rhevm	Tabla A.22, “RHEV-M REST API (RHEL 6.2 y versiones posteriores RHEV 3.0 y versiones posteriores)”
Cercado SCSI	fence_scsi	Tabla A.23, “Cercado SCSI”
Valla de VMware (Interfaz SOAP)	fence_vmware_soap	Tabla A.24, “Vallas de VMware (Interfaz SOAP) (Red Hat Enterprise Linux 6.2 y posterior)”
WTI Power Switch	fence_wti	Tabla A.25, “WTI Power Switch”

Tabla A.2, “Interruptor APC (telnet/SSH)” lista los parámetros de valla de dispositivos por **`fence_apc`**, el agente de valla para APC en telnet/SSH.

Tabla A.2. Interruptor APC (telnet/SSH)

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo APC conectado al clúster dentro del cual el demonio de valla ingresa a través de telnet/ssh.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto IP (opcional)	`ipport`	El puerto TCP a usar para conectar al dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Puerto	`port`	El puerto.
Interruptor (opcional)	`switch`	El número de interruptor para el interruptor APC que conecta al nodo cuando se tienen varios interruptores Daisy en cadena.
Usa SSH	`secure`	Indica que el sistema utilizará SSH para acceder al dispositivo.
Ruta al archivo de identidad SSH	`identity_file`	El archivo de identidad para SSH.

Tabla A.3, “Interruptor de alimentación APC en SNMP” lista los parámetros de dispositivo de valla utilizados por `fence_apc_snmp`, el agente de valla para APC que se registra en el dispositivo SNP a través del protocolo SNP.

Tabla A.3. Interruptor de alimentación APC en SNMP

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo APC conectado al clúster dentro del cual el demonio de valla ingresa vía el protocolo SNMP.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto UDP/TCP	`udpport`	El puerto UDP/TCP a usar para la conexión con el dispositivo, el valor predeterminado es 161.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Versión SNMP	`snmp_version`	La versión SNMP a usar (1, 2c, 3); el valor predeterminado es 1.
Comunidad SNMP	`community`	La cadena de comunidad SNMP, el valor predeterminado es `private`.
Nivel de seguridad SNMP	`snmp_sec_level`	El nivel de seguridad SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocolo de autenticación SNMP	`snmp_auth_prot`	El protocolo de autenticación SNMP (MD5, SHA).
Protocolo de privacidad SNMP	`snmp_priv_prot`	El protocolo de privacidad SNMP (DES, AES).
Contraseña de protocolo de privacidad SNMP	`snmp_priv_passwd`	La contraseña de protocolo de privacidad SNMP.
El script de protocolo de privacidad SNMP	`snmp_priv_passwd_script`	El script que proporciona una contraseña para el protocolo de privacidad SNMP. Su uso remplaza el parámetro **Contraseña de protocolo de privacidad SNMP**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Número de puerto (salida)	`port`	El puerto.

La Tabla A.4, “Interruptor Brocade Fabric” lista los parámetros de dispositivos de vallas utilizados por `fence_brocade`, el agente de vallas para interruptores Brocade FC.

Tabla A.4. Interruptor Brocade Fabric

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo Brocade conectado al clúster.
Dirección IP o nombre de host	`ipaddr`	La dirección IP asignada al dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Puerto	`port`	El número de salida de interruptor.

La Tabla A.5, “Cisco MDS” lista los parámetros de valla utilizados por `fence_cisco_mds`, el agente de valla para Cisco MDS.

Tabla A.5. Cisco MDS

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo series 9000 Cisco MDS con SNMP habilitado.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto UDP/TCP	`udpport`	El puerto UDP/TCP a usar para la conexión con el dispositivo, el valor predeterminado es 161.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Número de puerto (salida)	`port`	El puerto.
Versión SNMP	`snmp_version`	La versión SNMP a usar (1, 2c, 3).
Comunidad SNMP	`community`	La cadena de comunidad SNMP.
Nivel de seguridad SNMP	`snmp_sec_level`	El nivel de seguridad SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocolo de autenticación SNMP	`snmp_auth_prot`	El protocolo de autenticación SNMP (MD5, SHA).
Protocolo de privacidad SNMP	`snmp_priv_prot`	El protocolo de privacidad SNMP (DES, AES).
Contraseña de protocolo de privacidad SNMP	`snmp_priv_passwd`	La contraseña de protocolo de privacidad SNMP.
El script de protocolo de privacidad SNMP	`snmp_priv_passwd_script`	El script que proporciona una contraseña para el protocolo de privacidad SNMP. Su uso remplaza el parámetro **Contraseña de protocolo de privacidad SNMP**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.

La Tabla A.6, “Cisco UCS” lista los parámetros de dispositivo de valla utilizados por `fence_cisco_ucs`, el agente de valla para Cisco UCS.

Tabla A.6. Cisco UCS

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo Cisco UCS.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto IP (opcional)	`ipport`	El puerto TCP a usar para conectar al dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Usa SSL	`ssl`	Usa las conexiones SSL para comunicarse con el dispositivo.
Suborganización	`suborg`	Ruta adicional necesario para acceder a la organización.
Número de puerto (salida)	`port`	Nombre de la máquina virtual
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.

La Tabla A.7, “Dell DRAC 5” lista los parámetros de dispositivos de valla utilizados por `fence_drac5`, el agente de valla para Dell DRAC 5.

Tabla A.7. Dell DRAC 5

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	El nombre asignado al DRAC.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al DRAC.
Puerto IP (opcional)	`ipport`	El puerto TCP a usar para conectar al dispositivo.
El nombre de usuario	`login`	El nombre de usuario para acceder al DRAC
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al DRAC.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Usa SSH	`secure`	Indica que el sistema usa SSH para acceder el dispositivo.
Ruta al archivo de identidad SSH	`identity_file`	El archivo de identidad para SSH.
Nombre de módulo	`module_name`	(opcional) El nombre de módulo para el DRAC cuando se tienen varios módulos DRAC.
Forzar el indicador de comandos	`cmd_prompt`	El indicador de comandos a usar. El valor predeterminado es '\$'.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.

La Tabla A.8, "El controlador de energía de red Eaton (Controlador SNMP) (Red Hat Enterprise Linux 6.4 y posteriores)" lista los parámetros del dispositivo de valla utilizados por `fence_eaton_snmp`, el agente de valla para Eaton en el interruptor de energía de red SNMP.

Tabla A.8. El controlador de energía de red Eaton (Controlador SNMP) (Red Hat Enterprise Linux 6.4 y posteriores)

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el interruptor de red Eaton conectado al clúster.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto UDP/TCP (opcional)	`udpport`	El puerto UDP/TCP a usar para la conexión con el dispositivo, el valor predeterminado es 161.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Versión SNMP	`snmp_version`	La versión SNMP a usar (1, 2c, 3); el valor predeterminado es 1.
Comunidad SNMP	`community`	La cadena de comunidad SNMP, el valor predeterminado es `private`.
Nivel de seguridad SNMP	`snmp_sec_level`	El nivel de seguridad SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocolo de autenticación SNMP	`snmp_auth_prot`	El protocolo de autenticación SNMP (MD5, SHA).
Protocolo de privacidad SNMP	`snmp_priv_prot`	El protocolo de privacidad SNMP (DES, AES).
Contraseña de protocolo de privacidad SNMP	`snmp_priv_passwd`	La contraseña de protocolo de privacidad SNMP.
El script de protocolo de privacidad SNMP	`snmp_priv_passwd_script`	El script que proporciona una contraseña para el protocolo de privacidad SNMP. Su uso remplaza el parámetro **Contraseña de protocolo de privacidad SNMP**.
Power wait (segundos)	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Número de puerto (salida)	`port`	El número de conexión física o nombre de la máquina virtual. El parámetro es obligatorio.

La Tabla A.9, “Controlador Egenera SAN” lista los parámetros de dispositivos de vallas utilizados por `fence_egenera`, el agente de vallas para Egenera BladeFrame.

Tabla A.9. Controlador Egenera SAN

Campo luci	Atributo cluster.conf	Descripción
Nombre	**name**	Un nombre para el dispositivo Egenera BladeFrame conectado al clúster.
CServer	**cserver**	El nombre de host (y opcionalmente el nombre de usuario en la forma de **username@hostname**) asignado al dispositivo. Consulte la página de manual fence_egenera(8) para obtener mayor información.
Ruta ESH (opcional)	**esh**	La ruta al comando esh en el cserver (el predeterminado es /opt/pan- mgr/bin/esh)
Nombre de host	**user**	El nombre de ingreso. El valor predeterminado es **root**.
lpan	**lpan**	La red del área del proceso lógico (LPAN) del dispositivo.
pserver	**pserver**	LA cuchilla de procesamiento (pserver) del nombre del dispositivo.

La tabla Tabla A.10, “ePowerSwitch” lista los parámetros de dispositivos de vallas utilizados por **fence_eps**, el agente de dispositivos para ePowerSwitch.

Tabla A.10. ePowerSwitch

Campo luci	Atributo cluster.conf	Descripción
Nombre	**name**	Un nombre para el dispositivo ePowerSwitch conectado al clúster.
Dirección IP o nombre de host	**ipaddr**	La dirección IP o nombre de host asignado al dispositivo.
El nombre de usuario	**login**	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	**passwd**	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	**passwd_script**	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Nombre de página oculta	**hidden_page**	El nombre de la página oculta para el dispositivo.
Número de puerto (salida)	**port**	El número de conexión física o nombre de la máquina virtual.

La Tabla A.11, “Fence virt” lista los parámetros de dispositivos de vallas utilizados por **fence_virt**, el valor del agente de vallas para una dispositivo de vallas Fence virt.

Tabla A.11. Fence virt

Campo luci	Atributo cluster.conf	Descripción
Nombre	**name**	Un nombre para el dispositivo de valla Fence virt.
Dispositivo serial	**serial_device**	En el host, el dispositivo serial debe ser asignado en cada archivo de configuración de dominio. Para obtener mayor información, consulte la página de manual **fence_virt.conf**. Si este campo se especifica, es el agente de valla **fence_virt** que debe operar en modo serial. Al no especificar el valor el agente de valla **fence_virt** operará en modo de canal VM.
Parámetros seriales	**serial_params**	Los parámetros seriales. El predeterminado es 115200, 8N1.
Dirección IP de Canal VM	**channel_address**	El canal IP. El valor predeterminado es 10.0.2.179.
Puerto o Dominio (depreciado)	**port**	La máquina virtual (dominio UUID o nombre) para la valla.
	ipport	El puerto de canal. El valor predeterminado es 1229, el cual se utiliza para configurar el dispositivos de valla con **luci**.

La Tabla A.12, “Fujitsu Siemens Remoteview Service Board (RSB)” lista los parámetros de dispositivos de valla utilizados por **fence_rsb**, el agente de vallas para Fujitsu-Siemens RSB.

Tabla A.12. Fujitsu Siemens Remoteview Service Board (RSB)

Campo luci	Atributo cluster.conf	Descripción
Nombre	**name**	Un nombre para el RSB a usar como dispositivo de valla.
Dirección IP o nombre de host	**ipaddr**	El nombre de host asignado al dispositivo.
El nombre de usuario	**login**	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	**passwd**	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	**passwd_script**	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Puerto TCP	**ipport**	El número de puerto en el cual el servicio telnet escucha. El valor predeterminado es 3172.

La Tabla A.13, “HP BladeSystem (Red Hat Enterprise Linux 6.4 y posterior)” lista los parámetros de dispositivos de valla utilizados por **fence_hpblade**, el agente de vallas para HP BladeSystem.

Tabla A.13. HP BladeSystem (Red Hat Enterprise Linux 6.4 y posterior)

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	El nombre asignado al dispositivo HP Bladesystem conectado al clústerr.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host address or hostname assigned to the HP BladeSystem device.
Puerto IP (opcional)	`ipport`	El puerto TCP a usar para conectar al dispositivo.
El nombre de usuario	`login`	El nombre de inicio de sesión utilizado para acceder al dispositivo HP BladeSystem. Este parámetro es obligatorio.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo de valla.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Forzar el indicador de comandos	`cmd_prompt`	El indicador de comandos a usar. El valor predeterminado es '\$'.
Puerto faltante retorna OFF (apagado) en lugar de falla	`missing_as_off`	Puerto faltante retorna OFF (apagado) en lugar de falla.
Power wait (segundos)	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Usa SSH	`secure`	Indica que el sistema usa SSH para acceder el dispositivo.
Ruta al archivo de identidad SSH	`identity_file`	El archivo de identidad para SSH.

La Tabla A.14, "HP iLO/iLO2 (Integrated Lights Out)" lista los parámetros de dispositivos de valla utilizados por `fence_ilo`, el agente de vallas para dispositivos HP iLO.

Tabla A.14. HP iLO/iLO2 (Integrated Lights Out)

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el servidor con soporte HP iLO.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto IP (opcional)	`ipport`	Puerto TCP a usar para conectar con el dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.

La Tabla A.15, “HP iLO (Integrated Lights Out) MP” lista los parámetros de dispositivo de vallas utilizados por `fence_ilo_mp`, el agente de vallas para dispositivos HP iLO MP.

Tabla A.15. HP iLO (Integrated Lights Out) MP

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el servidor con soporte HP iLO.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto IP (opcional)	`ipport`	Puerto TCP a usar para conectar con el dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Usa SSH	`secure`	Indica que el sistema usa SSH para acceder el dispositivo.
Ruta al archivo de identidad SSH	`identity_file`	El archivo de identidad para SSH.
Forzar el indicador de comandos	`cmd_prompt`	El indicador de comandos a usar. El valor predeterminado es 'MP>', 'hpiLO->'.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.

La Tabla A.16, "IBM BladeCenter" lista los parámetros de dispositivo de vallas utilizados por `fence_bladecenter`, el agente de vallas para IBM BladeCenter.

Tabla A.16. IBM BladeCenter

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo IBM BladeCenter conectado al clúster.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto IP (opcional)	`ipport`	Puerto TCP a usar para conectar con el dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Usa SSH	`secure`	Indica que el sistema utilizará SSH para acceder al dispositivo.
Ruta al archivo de identidad SSH	`identity_file`	El archivo de identidad para SSH.

La Tabla A.17, “IBM BladeCenter SNMP” lista los parámetros de dispositivo de vallas utilizados por `fence_ibmblade`, el agente de vallas para IBM BladeCenter en SNMP.

Tabla A.17. IBM BladeCenter SNMP

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo IBM BladeCenter SNMP conectado al clúster.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto UDP/TCP (opcional)	`udpport`	Puerto UDP/TCP a usar para conexiones con el dispositivo; el valor predeterminado es 161.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Versión SNMP	`snmp_version`	La versión SNMP a usar (1, 2c, 3); el valor predeterminado es 1.
Comunidad SNMP	`community`	La cadena de comunidad SNMP.
Nivel de seguridad SNMP	`snmp_sec_level`	El nivel de seguridad SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocolo de autenticación SNMP	`snmp_auth_prot`	El protocolo de autenticación SNMP (MD5, SHA).
Protocolo de privacidad SNMP	`snmp_priv_prot`	El protocolo de privacidad SNMP (DES, AES).
Contraseña de protocolo de privacidad SNMP	`snmp_priv_passwd`	La contraseña de protocolo de privacidad SNMP
El script de protocolo de privacidad SNMP	`snmp_priv_passwd_script`	El script que proporciona una contraseña para el protocolo de privacidad SNMP. Su uso remplaza el parámetro **Contraseña de protocolo de privacidad SNMP**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Puerto	`port`	El número de conexión física o nombre de la máquina virtual.

La Tabla A.18, “IBM iPDU (Red Hat Enterprise Linux 6.4 y posterior)” lista los parámetros de dispositivos de valla utilizados por `fence_ipdu`, el agente de valla para iPDU sobre dispositivos SNMP.

Tabla A.18. IBM iPDU (Red Hat Enterprise Linux 6.4 y posterior)

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo IBM iPDU conectado al clúster dentro del cual el demonio de valla ingresa vía el protocolo SNMP.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto UDP/TCP	`udpport`	El puerto UDP/TCP a usar para la conexión con el dispositivo, el valor predeterminado es 161.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Versión SNMP	`snmp_version`	La versión SNMP a usar (1, 2c, 3); el valor predeterminado es 1.
Comunidad SNMP	`community`	La cadena de comunidad SNMP, el valor predeterminado es `private`.
Nivel de seguridad SNMP	`snmp_sec_level`	El nivel de seguridad SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocolo de autenticación SNMP	`snmp_auth_prot`	El protocolo de autenticación SNMP (MD5, SHA).
Protocolo de privacidad SNMP	`snmp_priv_prot`	El protocolo de privacidad SNMP (DES, AES).
Contraseña de protocolo de privacidad SNMP	`snmp_priv_passwd`	La contraseña de protocolo de privacidad SNMP.
El script de protocolo de privacidad SNMP	`snmp_priv_passwd_script`	El script que proporciona una contraseña para el protocolo de privacidad SNMP. Su uso remplaza el parámetro **Contraseña de protocolo de privacidad SNMP**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Puerto	`port`	El puerto.

La Tabla A.19, “IF MIB” lista los parámetros de dispsitivos utilizados por `fence_ifmib`, el agente de vallas para dispositivos IF-MIB.

Tabla A.19. IF MIB

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo IF MIB conectado al clúster.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto UDP/TCP (opcional)	`udpport`	El puerto UDP/TCP a usar para la conexión con el dispositivo, el valor predeterminado es 161.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Versión SNMP	`snmp_version`	La versión SNMP a usar (1, 2c, 3); el valor predeterminado es 1.
Comunidad SNMP	`community`	La cadena de comunidad SNMP.
Nivel de seguridad SNMP	`snmp_sec_level`	El nivel de seguridad SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocolo de autenticación SNMP	`snmp_auth_prot`	El protocolo de autenticación SNMP (MD5, SHA).
Protocolo de privacidad SNMP	`snmp_priv_prot`	El protocolo de privacidad SNMP (DES, AES).
Contraseña de protocolo de privacidad SNMP	`snmp_priv_passwd`	La contraseña de protocolo de privacidad SNMP.
El script de protocolo de privacidad SNMP	`snmp_priv_passwd_script`	El script que proporciona una contraseña para el protocolo de privacidad SNMP. Su uso remplaza el parámetro **Contraseña de protocolo de privacidad SNMP**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Puerto	`port`	El número de conexión física o nombre de la máquina virtual.

La Tabla A.20, “Intel Modular” lista los parámetros de dispositivos utilizados por `fence_intelmodular`, el agente de vallas para Intel Modular.

Tabla A.20. Intel Modular

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo Intel Modular conectado al clúster.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Versión SNMP	`snmp_version`	La versión SNMP a usar (1, 2c, 3); el valor predeterminado es 1.
Comunidad SNMP	`community`	La cadena de comunidad SNMP, el valor predeterminado es `private`.
Nivel de seguridad SNMP	`snmp_sec_level`	El nivel de seguridad SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocolo de autenticación SNMP	`snmp_auth_prot`	El protocolo de autenticación SNMP (MD5, SHA).
Protocolo de privacidad SNMP	`snmp_priv_prot`	El protocolo de privacidad SNMP (DES, AES).
Contraseña de protocolo de privacidad SNMP	`snmp_priv_passwd`	La contraseña de protocolo de privacidad SNMP.
El script de protocolo de privacidad SNMP	`snmp_priv_passwd_script`	El script que proporciona una contraseña para el protocolo de privacidad SNMP. Su uso remplaza el parámetro **Contraseña de protocolo de privacidad SNMP**.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Puerto	`port`	El número de conexión física o nombre de la máquina virtual.

La Tabla A.21, “LAN IPMI (Interfaz de administración de plataforma inteligente)” lists the fence device parameters used by `fence_ipmilan`, the fence agent for IPMI over LAN.

Tabla A.21. LAN IPMI (Interfaz de administración de plataforma inteligente)

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para un dispositivo LAN IPMI conectado al clúster.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
El nombre de usuario	`login`	El nombre de inicio del usuario que puede expedir comandos de apagado/encendido al puerto IPMI.
Contraseña	`passwd`	La contraseña para autenticar la conexión al puerto IPMI.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Tipo de autenticación	`auth`	Tipo de autenticación IPMI LAN: `none`, `password`, o `md5`.
Use Lanplus	`lanplus`	`True` o `1`. Si está en blanco, entonces el valor es `False`.
Ciphersuite a usar	`cipher`	El servidor remoto de autenticación, integridad y algoritmos de cifrado a usar para conexiones lanplus IPMIv2.
Nivel de Privilegio	`privlvl`	El nivel de privilegio en el dispositivo IPMI.

La Tabla A.22, “RHEV-M REST API (RHEL 6.2 y versiones posteriores RHEV 3.0 y versiones posteriores)” lista los parámetros de dispositivo de vallas utilizados por `fence_rhevm`, el agente de vallas para RHEV-M REST API.

Tabla A.22. RHEV-M REST API (RHEL 6.2 y versiones posteriores RHEV 3.0 y versiones posteriores)

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Nombre del dispositivo de valla RHEV-M REST API.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto IP (opcional)	`ipport`	Puerto TCP a usar para conectar con el dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Usa SSL	`ssl`	Usa las conexiones SSL para comunicarse con el dispositivo.
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Puerto	`port`	El número de conexión física o nombre de la máquina virtual.

La Tabla A.23, “Cercado SCSI” lista los parámetros de dispositivos de vallas utilizados por `fence_scsi`, el agente de vallas para reservaciones de SCSI persistente. reservations.

Nota

El uso de reservaciones SCSI persistentes como un método de valla se admite con las siguientes limitaciones:

- Cuando se usa el cercado SCSI, todos los nodos en el clúster deben registrarse con los mismos dispositivos para que cada nodo pueda remover otra clave de registro de nodo desde todos los dispositivos con los que está registrado.
- Los dispositivos utilizados para los volúmenes de clúster deben ser un LUN completo, no particiones. Las reservaciones SCSI persistentes funcionan en un LUN entero, lo que significa que el acceso está controlado para cada LUN, no para particiones individuales.

Tabla A.23. Cercado SCSI

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el dispositivo de vallas SCSI.
Nombre de nodo		
Llave para la acción actual		(anula nombre de nodo)

La Tabla A.24, “Vallas de VMware (Interfaz SOAP) (Red Hat Enterprise Linux 6.2 y posterior)” lista los parámetros de dispositivos de valla utilizados por **fence_vmware_soap**, el agente de vallas para VMWare en SOAP API.

Tabla A.24. Vallas de VMware (Interfaz SOAP) (Red Hat Enterprise Linux 6.2 y posterior)

Campo luci	Atributo cluster.conf	Descripción
Nombre	**name**	Un nombre para el dispositivo de valla Fence virt.
Dirección IP o nombre de host	**ipaddr**	La dirección IP o nombre de host asignado al dispositivo.
Puerto IP (opcional)	**ipport**	Puerto TCP a usar para conectar con el dispositivo.
El nombre de usuario	**login**	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	**passwd**	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	**passwd_script**	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Separador	**separator**	Separador para CSV creado por lista de operación. El valor predeterminado es una coma(,).
Espera de energía	**power_wait**	Número de segundos de espera después de expedir un comando de apagado o encendido.
Nombre de VM	**port**	Nombre de máquina virtual en el formato de ruta de inventario (por ejemplo, /datacenter/vm/Discovered_virtual_machine/myMachine).
VM UUID	**uuid**	El UUID de la máquina virtual para vallas.
Usa SSL	**ssl**	Usa las conexiones SSL para comunicarse con el dispositivo.

La Tabla A.25, “WTI Power Switch” lista los parámetros de dispositivos de vallas utilizados por **fence_wti**, el agente de vallas para el interruptor de energía de red WTI.

Tabla A.25. WTI Power Switch

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre para el interruptor WTI conectado al clúster.
Dirección IP o nombre de host	`ipaddr`	La dirección IP o nombre de host asignado al dispositivo.
Puerto IP (opcional)	`ipport`	El puerto TCP a usar para conectar al dispositivo.
El nombre de usuario	`login`	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	`passwd`	La contraseña utilizada para autenticar la conexión al dispositivo.
Script de contraseña (opcional)	`passwd_script`	El script que proporciona una contraseña para acceder al dispositivo de valla. Su uso remplaza el parámetro de **Contraseña**.
Puerto	`port`	El número de conexión física o nombre de la máquina virtual.
Forzar el indicador de comandos	`cmd_prompt`	El indicador de comandos a utilizar. El valor predeterminado es ['RSM>', '>MPC', 'IPS>', 'TPS>', 'NBB>', 'NPS>', 'VMR>']
Espera de energía	`power_wait`	Número de segundos de espera después de expedir un comando de apagado o encendido.
Usa SSH	`secure`	Indica que el sistema utilizará SSH para acceder al dispositivo.
Ruta al archivo de identidad SSH	`identity_file`	El archivo de identidad para SSH.

Parámetros de recursos de alta disponibilidad

Este apéndice proporciona descripciones de parámetros de recursos de alta disponibilidad. Puede configurar los parámetros con **luci**, mediante el comando **ccs** o editando **etc/cluster/cluster.conf**. La Tabla B.1, "Resumen de recursos de alta disponibilidad" lista los recursos, sus agentes de recursos correspondientes y referencias a otras tablas que contienen descripciones de parámetros. Para entender a los agentes de recursos en más detalle, puede verlos en **/usr/share/cluster** de cualquier nodo de clúster.

Además de los agentes de recurso descritos en este apéndice, el directorio **/usr/share/cluster** incluye un script básico para un grupo de recursos, **service.sh**. Para obtener mayor información sobre los parámetros incluidos en este script, consulte el propio script **service.sh**.

Para obtener una lista completa de una descripción de los elementos y atributos de **cluster.conf**, consulte el esquema de cluster en **/usr/share/cluster/cluster.rng**, y el esquema anotado en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (por ejemplo **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Tabla B.1. Resumen de recursos de alta disponibilidad

Recursos	Agente de recursos	Referencia para descripción de parámetros
Apache	apache.sh	Tabla B.2, “Servidor Apache”
Instancia de Condor	condor.sh	Tabla B.3, “Instancia de Condor”
Sistema de archivos	fs.sh	Tabla B.4, “Sistema de archivos”
Sistema de archivos GFS2	clusterfs.sh	Tabla B.5, “GFS2”
Dirección IP	ip.sh	Tabla B.6, “Dirección IP”
HA LVM	lvm.sh	Tabla B.7, “HA LVM”
MySQL	mysql.sh	Tabla B.8, “MySQL”
Cliente NFS	nfsclient.sh	Tabla B.9, “Cliente NFS”
NFS Export	nfsexport.sh	Tabla B.10, “NFS Export”
Servidor NFS	nfsserver.sh	Tabla B.11, “Servidor NFS”
Montaje NFS/CIFS	netfs.sh	Tabla B.12, “Montaje NFS/CIFS”
Open LDAP	openldap.sh	Tabla B.13, “Open LDAP”
Instancia de conmutación de Oracle 10g/11g	oracledb.sh	Tabla B.14, “Instancia de conmutación de Oracle 10g/11G”
Instancia de conmutación de Oracle 10g	orainstance.sh	Tabla B.15, “Instancia de conmutación de Oracle 10g”
Oyente de Oracle 10g	oralistener.sh	Tabla B.16, “Oyente de Oracle 10g”
PostgreSQL 8	postgres-8.sh	Tabla B.17, “PostgreSQL 8”
Base de datos SAP	SAPDatabase	Tabla B.18, “Base de datos SAP”
Instancia SAP	SAPInstance	Tabla B.19, “Instancia SAP”
Samba	samba.sh	Tabla B.20, “Servidor Samba”
Script	script.sh	Tabla B.21, “Script”
Sybase ASE	ASEHAagent.sh	Tabla B.22, “Instancia de conmutación Sybase ASE ”
Tomcat 6	tomcat-6.sh	Tabla B.23, “Tomcat 6”
Máquina virtual	vm.sh	Tabla B.24, “Máquina virtual” NOTA: **Luci** lo presenta como un servicio virtual si el clúster de host puede soportar máquinas virtuales.

Tabla B.2. Servidor Apache

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	**`name`**	El nombre del servicio Apache.
Root de servidor	**`server_root`**	El predeterminado es **`/etc/httpd`**.
Config File	**`config_file`**	Especifica el archivo de configuración Apache. El valor predeterminado **`/etc/httpd/conf`**.
Opciones httpd	**`httpd_options`**	Otras opciones de línea de comandos para **`httpd`**.
Espera de apagado (segundos)	**`shutdown_wait`**	Especifica el número de segundos de espera para el final correcto de apagado del servicio.

Tabla B.3. Instancia de Condor

Campo	Campo luci	Atributo `cluster.conf`
Nombre de instancia	**`name`**	Especifica un nombre único para la instancia de Condor.
Tipo de subsistema de Condor	**`type`**	Especifica el tipo de subsistema de Condor para esta instancia: **`schedd`**, **`job_server`**, o **`query_server`**.

Tabla B.4. Sistema de archivos

Campo luci	Atributo cluster.conf	Descripción

Campo luci	Atributo cluster.conf	Descripción

Campo luci	Atributo cluster.conf	Descripción

Campo luci	Atributo cluster.conf	Descripción
Nombre	**name**	Especifica un nombre para el recurso de sistema de archivos.
Tipo de sistema de archivos	**fstype**	Si no está especificado, **mount** intenta determinar el tipo de sistema de archivos.
Punto de montaje	**mountpoint**	Ruta en jerarquía de sistema de archivos para montar este sistema de archivos.
Dispositivo, etiqueta FS o UUID	**device**	Especifica el dispositivo asociado con el recurso del sistema de archivos. Este puede ser un dispositivo de bloque, una etiqueta de sistema de archivos o UUID del sistema de archivos.
Opciones de montaje	**options**	Opciones de montaje; es decir, opciones utilizadas cuando se monta el sistema de archivos. Estas puede ser específicas al sistema de archivos. Consulte la página del manual ***mount(8)*** para ver las opciones de montaje soportadas.
ID de sistema de archivos (opcional)	**fsid**	**Nota** ***ID de sistema de archivos*** utilizado únicamente por servicios NFS. Al crear un nuevo recurso de sistema de archivos, puede dejar este campo en blanco. Si deja este campo en blanco, el ID del sistema de archivos será asignado automáticamente después de enviar el parámetro durante la configuración. Si necesita asignar un ID de sistema de archivos explícitamente, especifíquelo en este campo.
Forzar desmonte	**force_unmount**	Si está habilitado, obliga al sistema de archivos a desmontarse. La configuración predeterminada es ***desactivada***. ***Forzar el desmonte*** mata todos los procesos con el punto de montaje para liberar el montaje cuando intenta desmontar.
Forzar fsck	**force_fsck**	Si está habilitado, hace que **fsck** se ejecute en el sistema de archivos antes de montarlo. La configuración predeterminada es ***desactivado***.
Habilite el demonio NFS y la solución 'lockd' (Red Hat Enterprise Linux 6.4 y posterior)	**nfsrestart**	Si su sistema de archivos se exporta a través de NFS y en ocasiones no se puede desmontar (ya sea durante el apagado o la reubicación del servicio), esta opción bajará todas las referencias del sistema de archivos antes del desmontaje. Esta opción requiere que usted active la opción **Forzar el desmontaje** y no debe ser utilizada junto con el recurso del **Servidor NFS**. Se aconseja que establezca esta opción como último recurso, ya que es difícil intentar desmontar un sistema de archivos.
Usa revisiones de estatus rápidas	**quick_status**	Si está activada, realiza revisiones de estatus rápidas.
Reiniciar nodo de host si el desmonte falla	**self_fence**	

Campo luci	Atributo `cluster.conf`	Descripción
		SI está habilitado, reinicie el nodo en caso de que el desmontaje del sistema de archivos falle. El agente de recursos **`filesystem`** acepta un valor de 1, **`yes`**, **`on`**, o **`true`** para habilitar el parámetro y un valor de 0, **`no`**, **`off`**, o **`false`** para desactivarlo. El parámetro predeterminado es ***`disabled`***.

Tabla B.5. GFS2

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	El nombre del recurso del sistema de archivos.
Punto de montaje	`mountpoint`	La ruta en la cual se monta el recurso del sistema de archivos
Dispositivo, etiqueta FS o UUID	`device`	El archivo de dispositivo asociado con el recurso del sistema de archivos.
Tipo de sistema de archivos	`fstype`	Establecer a GFS2 en **luci**
Opciones de montaje	`options`	Opciones de montaje.
ID de sistema de archivos (opcional)	`fsid`	**Nota** ***ID de sistema de archivos*** utilizado únicamente por servicios NFS. Al crear un nuevo recurso GFS2, puede dejar este campo en blanco. Si deja el campo en blanco el ID del sistema de archivos se asigna automáticamente después de enviar el parámetro durante la configuración. Si necesita asignar un ID de sistema de archivos explícitamente, especifíquelo en este campo.
Forzar desmonte	`force_unmount`	Si está habilitado, obliga al sistema de archivos a desmontarse. El valor predeterminado es ***desactivado***. El parámetro ***Forzar desmonte*** mata todos los procesos mediante un punto de montaje para liberar e montaje cuando trate de desmontarse. Con recurso GFS2, el punto de montaje *no* se desmonta en ruptura de servicio a menos que ***Forzar desmonte*** esté *habilitado*.
Habilite el demonio NFS y la solución 'lockd' (Red Hat Enterprise Linux 6.4 y posterior)	`nfsrestart`	Si su sistema de archivos se exporta a través de NFS y en ocasiones no se puede desmontar (ya sea durante el apagado o la reubicación del servicio), esta opción bajará todas las referencias del sistema de archivos antes del desmontaje. Esta opción requiere que usted active la opción **`Forzar el desmontaje`** y no debe ser utilizada junto con el recurso del **`Servidor NFS`**. Se aconseja que establezca esta opción como último recurso, ya que es difícil intentar desmontar un sistema de archivos.
Reiniciar nodo de host si el desmonte falla	`self_fence`	Si está habilitado, el desmontaje del sistema de archivos fallará, el nodo se reiniciará inmediatamente . Por lo general, se utiliza junto con el soporte de force-unmount, pero no se requiere. El agente de recursos **`GFS2`** acepta un valor de 1, **`yes`**, **`on`**, o **`true`** para habilitar este parámetro, y un valor de 0, **`no`**, **`off`**, o **`false`** para inhabilitarlo.

Tabla B.6. Dirección IP

Campo luci	Atributo `cluster.conf`	Descripción
Dirección IP y bits de máscara de red (Netmask)	`address`	La dirección IP (y, opcionalmente, bits de Netmask) para el recurso. Bits de Netmask o longitud de prefijo de red, puede ir después de la dirección con una barra inclinada como separador, cumpliendo con la anotación CIDR (por ejemplo, 10.1.1.1/8). Esta es una dirección IP virtual. Las direcciones IPv4 e IPv6 tienen soporte, como en monitorización de enlaces NIC para cada dirección IP.
Enlace de monitor	`monitor_link`	Al habilitarlo hace que el estatus falle si el enlace de la NIC, al cual está enlazado esta dirección IP, no está presente.
Inhabilita actualizaciones para rutas estáticas	`disable_rdisc`	Inhabilita actualizaciones de rutas mediante protocolo RDISC.
Número de segundos dormido tras retirar una dirección IP	`sleeptime`	Especifica la cantidad de tiempo (en segundos) para dormir.

Tabla B.7. HA LVM

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Un nombre único para este recurso LVM.
Nombre de grupo de volúmenes	`vg_name`	Un nombre descriptivo del grupo de volúmenes que está siendo administrado.
Nombre de volumen lógico (opcional)	`lv_name`	Nombre del volumen lógico que está siendo administrado. Este parámetro es opcional, si hay más de un volumen lógico en el grupo de volúmenes que se está administrando.
Cercar el nodo si está habilitado para etiquetas Clean UP LVM	`self_fence`	Cerque el nodo si no puede limpiar las etiquetas LVM. El agente de recursos LVM acepta un valor de 1 o `yes` para habilitar este parámetro, y un valor de 0 o `no` para desactivarlo.

Tabla B.8. MySQL

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Especifica un nombre de recurso de servidor MySQL.
Config File	`config_file`	Especifica el archivo de configuración. El valor predeterminado es `/etc/my.cnf`.
Dirección de escucha	`listen_address`	Especifica una dirección para el servicio MySQL. Si no se proporciona una dirección IP, se tomará la primera dirección IP del servicio.
Opciones mysqld	`mysqld_options`	Otras opciones de línea de comandos para `httpd`.
Espera de inicio (segundos)	`startup_wait`	Especifica el número de segundos de espera para el final correcto del inicio del servicio.
Espera de apagado (segundos)	`shutdown_wait`	Especifica el número de segundos de espera para el final correcto de apagado del servicio.

Tabla B.9. Cliente NFS

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Este es un nombre simbólico de un cliente utilizado para referirse al cliente en el árbol de recursos. *No* es lo mismo que la opción ***`Target`***.
Nombre de host de destino, comodín o Netgroup	`target`	Es el servidor desde el cual usted está montando. Puede especificarse mediante un nombre de host, un comodín (dirección IP o basado en nombre de host) o un grupo de red que define un host o hosts para exportarlos.
Permitir recuperación de este cliente NFS	`allow_recover`	Permitir recuperación.
Opciones	`options`	Define una lista de opciones para este cliente — por ejemplo, los derechos de acceso de cliente adicional. Para obtener mayor información, consulte la página del manual ***`exports`*** *(5), General Options*.

Tabla B.10. NFS Export

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Nombre descriptivo del recurso. El recurso de exportación de NFS asegura que todos los demonios NFS estén ejecutándose. Si son reutilizables completamente, solo se necesitará un recurso de exportación NFS. **Consejo** Nombre de recurso de exportación de NFS para que puede distinguirse claramente desde otros recurso NFS.

Tabla B.11. Servidor NFS

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Nombre descriptivo del recurso de servidor NFS. El recurso de servidor NFS sirve para exportar sistemas de archivos NFSv4 a los clientes. Debido a la forma como funciona NFSv4, únicamente el recurso NFSv4 puede existir en un servidor a la vez. Además, no es posible utilizar el recurso de servidor NFS cuando también se están utilizando las instancias locales de NFS en cada nodo de clúster.

Tabla B.12. Montaje NFS/CIFS

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Nombre simbólico para el montaje NFS o CIFS. **Nota** Este recurso se requiere solamente cuando se configura un servicio de clúster para que sea un cliente NFS.
Punto de montaje	`mountpoint`	Ruta en la cual el sistema de archivos será montado.
Host	`host`	Dirección IP de servidor NFS/CIFS o nombre de host.
Nombre de directorio de exportación de NFS o nombre de recurso compartido de CIFS.	`export`	Nombre de directorio de exportación de NFS o nombre de recurso compartido de CIFS.
Tipo de sistema de archivos:	`fstype`	Tipo de sistema de archivos: » ***NFS3*** — Especifica el uso de la versión de NFS. Esta es la configuración predeterminada. » ***NFS4 v4*** — Especifica el uso del protocolo NFSv4. » ***CIFS*** — Especifica el uso del protocolo CIFS.
Forzar desmonte	`force_unmount`	Si ***Forzar desmonte*** está habilitado, el clúster mata todos los procesos mediante este sistema de archivos cuando se detiene el servicio. Al matar todos los procesos mediante el sistema de archivos se libera el sistema de archivos. De lo contrario, el desmonte fallará, y se reiniciará el servicio.
No desmonte el sistema de archivos durante una parada de la operación de reubicación.	`no_unmount`	Si está activado, especifica que el sistema de archivos no debe ser desmontado durante una operación de parada o reubicación.
Opciones	`options`	Opciones de montaje. Especifica una lista de opciones de montaje. Si no se especifica ninguna, el sistema se monta `-o sync`.

Tabla B.13. Open LDAP

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Especifica un nombre de servicio para registro y otros propósitos.
Config File	`config_file`	Especifica una ruta absoluta a un archivo de configuración. El valor predeterminado es `/etc/openldap/slapd.conf`.
Lista URL	`url_list`	El valor predeterminado es `ldap:///`.
Opciones `slapd`	`slapd_options`	Otras opciones de línea de comandos para `slapd`.
Espera de apagado (segundos)	`shutdown_wait`	Especifica el número de segundos de espera para el final correcto de apagado del servicio.

Tabla B.14. Instancia de conmutación de Oracle 10g/11G

Campo luci	Atributo `cluster.conf`	Descripción
Nombre de instancia (SID) de instancia de Oracle	`name`	Nombre de instancia.
Nombre de usuario de Oracle	`user`	Este es el nombre de usuario del usuario de Oracle con el que la instancia AS de Oracle se ejecuta.
Directorio principal de aplicación de Oracle	`home`	Este es el directorio principal de Oracle (aplicación, no usuario). Se configura durante la instalación de Oracle.
Tipo de autenticación de Oracle	`type`	El tipo de instalación de Oracle. Predeterminado: `10g`, Instancia de base de datos y `base` de Oyente únicamente , base de datos, Oyente, Gestor de empresas, e ISQL*Plus: `base -em` (o `10g`), o Servidor de aplicación de Internet (infraestructura): `ias` (o `10g-ias`).
Nombre de host virtual (opcional)	`vhost`	El nombre de host virtual coincidente con el nombre de host de instalación de Oracle 10g. Observe que durante el inicio/parada de un recurso oracledb, su nombre de host se cambia temporalmente a este nombre de host. Por lo tanto, debe configurar un recurso oracledb como parte de un servicio exclusivo únicamente.

Tabla B.15. Instancia de conmutación de Oracle 10g

Campo luci	Atributo `cluster.conf`	Descripción
Nombre de instancia (SID) de instancia de Oracle	**`name`**	Nombre de instancia.
Nombre de usuario de Oracle	**`user`**	Este es el nombre de usuario del usuario de Oracle con el que la instancia de Oracle se ejecuta.
Directorio principal de aplicación de Oracle	**`home`**	Este es el directorio principal de Oracle (aplicación, no usuario). Se configura durante la instalación de Oracle.
Lista de los oyentes de Oracle (opcional, separados por espacios)	**`listeners`**	Lista de oyentes de Oracle que iniciarán con la instancia de base de datos. Los nombres de oyentes están separados por espacios en blanco. Se predetermina a vacío lo cual desactiva oyentes.
Ruta para el archivo Lock (opcional)	**`lockfile`**	Sitio para lockfile que será utilizado para revisar si Oracle está ejecutándose o no. Se predetermina al sitio en **`/tmp`**.

Tabla B.16. Oyente de Oracle 10g

Campo luci	Atributo `cluster.conf`	Descripción
Nombre de oyente	**`name`**	Nombre de oyente
Nombre de usuario de Oracle	**`user`**	Este es el nombre de usuario del usuario de Oracle con el que la instancia de Oracle se ejecuta.
Directorio principal de aplicación de Oracle	**`home`**	Este es el directorio principal de Oracle (aplicación, no usuario). Se configura durante la instalación de Oracle.

Tabla B.17. PostgreSQL 8

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Especifica un nombre de servicio para registro y otros propósitos.
Config File	`config_file`	Definir ruta absoluta para archivo de configuración. El valor predeterminado es `/var/lib/pgsql/data/postgresql.conf`.
Usuario Postmaster	`postmaster_user`	Usuario que ejecuta el servidor de base de datos porque puede ser ejecutado por root. El valor predeterminado es postgres.
Opciones Postmaster	`postmaster_options`	Otras opciones de línea de comando para Postmaster.
Espera de apagado (segundos)	`shutdown_wait`	Especifica el número de segundos de espera para el final correcto de apagado del servicio.

Tabla B.18. Base de datos SAP

Campo luci	Atributo `cluster.conf`	Descripción
Nombre de base de datos SAP	`SID`	Especifica un identificador de sistema único SAP. Por ejemplo, P01.
Directorio ejecutable SAP	`DIR_EXECUTABLE`	Especifica la ruta totalmente calificada para `sapstartsrv` y `sapcontrol`.
Tipo de base de datos	`DBTYPE`	Especifica uno de los siguientes tipos de base de datos: Oracle, DB6 o ADA.
Nombre de oyente de Oracle	`NETSERVICENAME`	Especifica nombre de oyente TNS de Oracle.
La pila ABAP no está instalada, solo la pila de Java lo está	`DBJ2EE_ONLY`	Si no tiene una pila de ABAP instalada en la base de datos SAP, habilite este parámetro.
Monitorización de nivel de aplicación	`STRICT_MONITORING`	Activa monitorización del nivel de aplicación
Inicia este servicio automáticamente	`AUTOMATIC_RECOVER`	Activa o desactiva la recuperación de inicio automática.
Ruta a Java SDK	`JAVE_HOME`	Ruta a Java SDK.
Nombre de archivo del controlador de JDBC	`DB_JARS`	Nombre de archivo del controlador JDBC.
Ruta al script de preinicio	`PRE_START_USEREXIT`	Ruta al script de preinicio.
Ruta al script de postinicio	`POST_START_USEREXIT`	Ruta al script de postinicio.
Ruta al script de pre-parada	`PRE_STOP_USEREXIT`	Ruta al script de pre-parada
Ruta al script de postparada	`POST_STOP_USEREXIT`	Ruta al script de postparada
Directorio Bootstrap de Instancia J2EE	`DIR_BOOTSTRAP`	El directorio bootstrap de instancia J2EE de ruta totalmente calificada. Por ejemplo, `/usr/sap/P01/J00/j2ee/cluster/bootstrap`.
Ruta de almacenaje de seguridad J2EE	`DIR_SECSTORE`	El directorio de la ruta de almacenaje de seguridad J2EE totalmente calificada. Por ejemplo, `/usr/sap/P01/SYS/global/security/lib/tools`.

Tabla B.19. Instancia SAP

Campo luci	Atributo `cluster.conf`	Descripción
Nombre de instancia SAP	`InstanceName`	El nombre de instancia totalmente calificado. Por ejemplo, 01_DVEBMGS00_sapp01ci.
Directorio ejecutable SAP	`DIR_EXECUTABLE`	La ruta totalmente calificada para `sapstartsrv` y `sapcontrol`.
Directorio que contiene el perfil SAP START	`DIR_PROFILE`	La ruta totalmente calificada al perfil SAP START.
Nombre del perfil SAP START	`START_PROFILE`	Especifica el nombre del perfil SAP START.
Número de segundos de espera antes de revisar estatus de inicio	`START_WAITTIME`	Especifica el número de segundos de espera antes de revisar el estatus de inicio (no espere a J2EE-Addin).
Activar recuperación de inicio automática	`AUTOMATIC_RECOVER`	Activa o desactiva la recuperación de inicio automática.
Ruta al script de preinicio	`PRE_START_USEREXIT`	Ruta al script de preinicio.
Ruta al script de postinicio	`POST_START_USEREXIT`	Ruta al script de postinicio.
Ruta al script de pre-parada	`PRE_STOP_USEREXIT`	Ruta al script de pre-parada
Ruta al script de postparada	`POST_STOP_USEREXIT`	Ruta al script de postparada

Nota

Con respecto a la Tabla B.20, “Servidor Samba”, cuando se crea o edita un servicio de clúster, conecte un recurso de servicio de Samba directamente al servicio, *no* a un recurso dentro de un servicio.

Tabla B.20. Servidor Samba

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Especifica el nombre del servidor de Samba.
Config File	`config_file`	Archivo de configuración de Samba
Otras opciones de línea de comandos para smbd	`smbd_options`	Otras opciones de línea de comandos para smbd.
Otras opciones de línea de comandos para nmbd.	`nmbd_options`	Otras opciones de línea de comandos para nmbd.
Espera de apagado (segundos)	`shutdown_wait`	Especifica el número de segundos de espera para el final correcto de apagado del servicio.

Tabla B.21. Script

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	`name`	Especifica un nombre para el script personalizado de usuario. El recurso de script permite que un script de inicio sea compatible con un LSB estándar que se utiliza para iniciar el servicio en clúster.
Ruta completa al archivo de script	`file`	Ingrese la ruta donde este script personalizado se localiza (por ejemplo, `/etc/init.d/`***`userscript`***).

Tabla B.22. Instancia de conmutación Sybase ASE

Campo luci	Atributo cluster.conf	Descripción
Nombre de instancia	`name`	Especifica el nombre de instancia del recurso Sybase ASE.
Nombre de servidor ASE	`server_name`	El nombre de servidor ASE que está configurado para el servidor de alta disponibilidad.
Directorio principal de SYBASE	`sybase_home`	El directorio principal de productos Sybase.
Archivo de registro	`login_file`	La ruta completa del archivo de registro que contiene el par: nombre de usuario y contraseña.
Archivo de interfaces	`interfaces_file`	La ruta completa de archivo de interfaces que se utiliza para iniciar o acceder el servido ASE.
Nombre de directorio SYBASE_ASE	`sybase_ase`	El nombre de directorio bajo sybase_home donde los productos ASE están instalados.
Nombre de directorio SYBASE_OCS	`sybase_ocs`	El nombre de directorio bajo sybase_home donde se instalan productos de OCS. Por ejemplo, ASE-15_0.
Usuario Sybase	`sybase_user`	El usuario que puede ejecutar el servidor ASE.
Iniciar tiempo de espera (segundos)	`start_timeout`	Valor de tiempo de espera de inicio.
Tiempo de espera de apagado (segundos)	`shutdown_timeout`	Valor de tiempo de espera de apagado.
Tiempo de espera de sondeo profundo	`deep_probe_timeout`	El máximo de segundos de espera para la respuesta del servidor ASE antes de determinar que el servidor no tuvo respuesta mientras se ejecuta un sondeo profundo.

Tabla B.23. Tomcat 6

Campo luci	Atributo cluster.conf	Descripción
Nombre	`name`	Especifica un nombre de servicio para registro y otros propósitos.
Config File	`config_file`	Especifica la ruta absoluta al archivo de configuración. El valor por defecto es `/etc/tomcat6/tomcat6.conf`.
Espera de apagado (segundos)	`shutdown_wait`	Especifica el número de segundos de espera para que se termine correctamente el servicio de apagado. El valor predeterminado es 30.

Importante

Respecto a la Tabla B.24, “Máquina virtual”, al configurar su clúster con recursos de máquina virtual, debe usar las herramientas de **`rgmanager`** para iniciar y detener las máquinas virtuales. El uso de **`virsh`** para iniciar la máquina puede hacer que la máquina virtual se ejecute en más de un sitio lo cual puede corromper los datos en la máquina virtual. Para obtener información sobre cómo configurar su sistema para reducir las posibilidades de que los administradores accidentalmente "inicien en doble" las máquinas virtuales al usar herramientas de clúster y no clúster, consulte la Sección 2.14, “Configuración de las máquinas virtuales en un entorno en clúster.”.

Nota

Los recursos de máquina virtual se configuran de forma diferente a la de otros recursos de clúster. Para configurar un recurso de máquina virtual con **luci**, añada un grupo de servicio al clúster, luego añada un recurso al servicio, seleccione **`Virtual Machine`** como el tipo de recursos e ingrese los parámetros de recursos de máquina virtual. Para obtener información sobre cómo configurar una máquina virtual con el comando **`ccs`**, consulte la Sección 5.12, “Recursos de máquinas virtuales”.

Tabla B.24. Máquina virtual

Campo luci	Atributo cluster.conf	Descripción

Campo luci	Atributo cluster.conf	Descripción

Campo luci	Atributo cluster.conf	Descripción

Campo luci	Atributo cluster.conf	Descripción
Nombre de servicio	**name**	Especifica el nombre de la máquina virtual. Al usar la interfaz de **luci**, especifíquela como un nombre de servicio.
Inicia este servicio automáticamente	**autostart**	Si está habilitada, esta máquina virtual se iniciará automáticamente después de que el clúster forme un cuórum. Si este parámetro está *desactivado*, esta máquina virtual *no* iniciará automáticamente después de que el clúster forme un cuórum. la máquina virtual es puesta en el estado ***desactivado***.
Ejecución exclusiva	**exclusive**	Si se habilita, esta máquina virtual solamente puede ser reubicada para ejecutarse en otro nodo de forma exclusiva; es decir, para que se ejecute en un nodo que no tenga otras máquinas virtuales ejecutándose en él. Si no hay nodos disponibles para que una máquina virtual se ejecuten exclusivamente, la máquina virtual no se reiniciará después de un fallo. Además, otras máquinas virtuales no se reubican automáticamente en un nodo que ejecute esta máquina virtual como ***Ejecutar exclusivo***. Puede anular esta opción si inicia en forma manual o reubica operaciones.
Dominio de conmutación	**domain**	Define listas de miembros de clúster para intentar en caso de que la máquina virtual falle.
Política de recuperación.	**recovery**	***Política de recuperación*** proporciona las opciones siguientes: • ***Inhabilitar*** — Desactiva la máquina virtual si falla. • ***Reubicar*** — Intenta reiniciar la máquina virtual en otro nodo; es decir, no intentará de reiniciar en el nodo actual. • ***Reiniciar*** — Intenta reiniciar la máquina virtual localmente (en el nodo actual) antes de reubicar (predeterminada) a la máquina virtual en otro nodo. • ***Reiniciar-Inhabilitar*** — El servicio se reiniciará en el lugar si se presenta un error. Sin embargo, si al reiniciar el servicio falla el servicio se desactivará en lugar de desplazarse a otro host en el clúster.
Opciones de reinicio	**max_restarts**, **restart_expire_time**	Si selecciona **Reiniciar** o **Reiniciar-Inhabilitar** como política de recuperación para el servicio, especifique el número máximo de fallas de reinicio antes de reubicar o desactivar el servicio y especificar el tiempo en segundos después del cual olvida reiniciar.
Tipo de migración	**migrate**	Especifica un tipo de migración de ***viva*** o ***pausa***. La configuración predeterminada en ***viva***.
Asignación de migración	**migration_mapping**	Especifica una interfaz alternativa para migrar. Especifíquela cuando, por ejemplo, la dirección de red utilizada para migrar máquina virtual en un nodo difiere de la dirección del nodo utilizado para comunicación de clúster. Especificar lo siguiente indica que cuando migra una máquina virtual de **member** a **member2**, en realidad migra a **target2**. Igualmente, cuando migra de **member2** a **member**, usted migra mediante **target**. **member:target,member2:target2**
Programa de	**status_pro**	

Campo luci	Atributo `cluster.conf`	Descripción
estatus	`gram`	Programa de estatus para ejecutar además de la revisión estándar para la presencia de una máquina virtual. Si se especifica, el programa de estatus se ejecuta una vez por minuto. Esto le permite determinar el estatus de servicios críticos dentro de una máquina virtual. Por ejemplo, si una máquina virtual ejecuta un servidor de red, su programa de estatus podría verificar si un servidor de red está activado y en ejecución; si la revisión de estatus falla (se indica al retornar un valor de no cero), la máquina virtual es recuperada. Después de iniciar la máquina virtual, el agente de recursos de máquina virtual llamará periódicamente al programa de estatus y esperará un código de retorno correcto (cero) antes de retornar. El programa se detendrá después de cinco minutos.
Ruta al archivo XML utilizado para crear la máquina virtual (VM)	`xmlfile`	Ruta completa al archivo XML `libvirt` que contiene la definición de dominio `libvirt`.
Ruta a los archivos de configuración de Máquina Virtual	`path`	Una especificación de ruta delimitada por dos puntos que el agente de recursos de máquina virtual (`vm.sh`) busca para el archivo de configuración de máquina virtual. Por ejemplo: `/mnt/guests/config:/etc/libvirt/qemu`. **Importante** La ruta *nunca* debe señalar directamente un archivo de máquina virtual.
Ruta al directorio de instantáneas de Máquina Virtual	`snapshot`	Ruta al directorio de instantáneas donde se almacenará la imagen de máquina virtual.
Hipervisor URI	`hypervisor_uri`	Hipervisor URI (normalmente automático).
URI de migración	`migration_uri`	URI de migración (normalmente automática).
Datos de túnel en ssh durante migración	`tunnelled`	Datos de túnel en ssh durante migración.

Comportamiento de recursos de alta disponibilidad

Este apéndice describe el comportamiento común de recursos de alta disponibilidad. Provee información suplementaria que puede ser útil en la configuración de servicios de alta disponibilidad. Puede configurar los parámetros con **Luci** o al editar `etc/cluster/cluster.conf`. Para obtener descripciones de parámetros de recursos de alta disponibilidad, consulte el Apéndice B, *Parámetros de recursos de alta disponibilidad*. Para entender los agentes de recurso en más detalle puede verlos en `/usr/share/cluster` de cualquier nodo de clúster.

Nota

Para comprender totalmente la información en este apéndice, requerirá entender en detalle los agentes de recursos y el archivo de configuración de clúster, `/etc/cluster/cluster.conf`.

Un servicio de alta disponibilidad es un grupo de recursos de clúster configurado dentro de una entidad coherente que proporciona servicios especializados a clientes. Un servicio de alta disponibilidad se representa como un árbol de recursos en el archivo de configuración de clúster, `/etc/cluster/cluster.conf` (en cada nodo de clúster). En el archivo de configuración de cluster, cada árbol de recursos es una representación XML que especifica cada recurso, sus atributos y su relación con otros recursos en el árbol de recursos (relación de padre, hijos y hermanos).

Nota

Puesto que un servicio de alta disponibilidad consiste en recursos organizados dentro de un árbol jerárquico, el servicio se conoce algunas veces como *árbol de recursos* o *grupo de recursos*. Ambos nombres son sinónimos de *servicio de alta disponibilidad*.

En la raíz de cada árbol de recursos hay un tipo especial de recurso— un *recurso de servicio*. Otros tipos de recursos comprenden el resto de un servicio que determina sus características. La configuración de un servicio de alta disponibilidad consiste en la creación de un recurso de servicio, la creación de recursos de clúster subordinados y su organización dentro de una entidad coherente conforme a las restricciones jerárquicas del servicio.

Este apéndice consta de las siguientes secciones:

- La Sección C.1, “Relaciones padre, hijo y hermanos entre recursos”
- La Sección C.2, “Solicitud de inicio para hermanos y solicitud de hijo de recursos”
- La Sección C.3, “Herencia, los "recursos" Bloques y reutilización de recursos”
- La Sección C.4, “Recuperación de fallas y subárboles independientes”
- La Sección C.5, “Depuración y prueba de servicios y ordenamiento de recursos”

Nota

Las secciones a continuación presentan ejemplos del archivo de configuración de clúster, `/etc/cluster/cluster.conf`, únicamente con propósitos de ilustración.

C.1. Relaciones padre, hijo y hermanos entre recursos

Un servicio de clúster es una entidad integrada que se ejecuta bajo el control de `rgmanager`. Todos los recursos en un servicio se ejecutan en el mismo nodo. Desde la perspectiva del `rgmanager`, un servicio de clúster es una entidad que puede ser iniciada, detenida o reubicada. No obstante, dentro de un servicio de clúster, la jerarquía de los recursos determina el orden en el cual cada recurso es iniciado o detenido. Los niveles jerárquicos constan de padre, hijo y hermano.

Ejemplo C.1, “Jerarquía de recursos del servicio foo” muestra un árbol de recursos de muestra del servicio *foo*. En el ejemplo, las relaciones entre los recursos son las siguientes:

- `fs:myfs` (<fs name="myfs" ...>) y `ip:10.1.1.2` (<ip address="10.1.1.2 .../>) son hermanos.
- `fs:myfs` (<fs name="myfs" ...>) es el padre de `script:script_child` (<script name="script_child"/>).
- `script:script_child` (<script name="script_child"/>) es el hijo de `fs:myfs` (<fs

name="myfs" ...>).

Ejemplo C.1. Jerarquía de recursos del servicio foo

```
<service name="foo" ...>
    <fs name="myfs" ...>
        <script name="script_child"/>
    </fs>
    <ip address="10.1.1.2" .../>
</service>
```

Las siguientes reglas se aplican a las relaciones padre e hijo en un árbol de recursos:

- Los padres se inician antes de los hijos.
- Todos los hijos deben detenerse para que el padre pueda detenerse.
- Para que un recurso se considere en buen estado de salud, todos sus hijos deben tener buena salud.

C.2. Solicitud de inicio para hermanos y solicitud de hijo de recursos

El recurso del servicio determina el orden de inicio y de parada de un recurso hijo dependiendo de si designa un atributo de tipo hijo a un recurso hijo así:

- Designa el atributo tipo-hijo (recurso de hijo *tipificado*) — Si el recurso de servicio designa un atributo tipo-hijo para un recurso de hijo, el recurso de hijo es *tipificado*. El atributo tipo-hijo explícitamente determina el orden de inicio y de parada del recurso hijo.
- *No designa* atributo tipo-hijo (recurso de hijo *no-tipificado*) — Si el recurso de servicios *no designa* un atributo tipo-hijo para un recurso de hijo, el recurso de hijo es *no-tipificado*. El recurso de servicio no controla explícitamente el orden de inicio y parada de un recurso de hijo no-tipificado. Si embargo, un recurso de hijo no-tipificado se inicia y se detiene según el orden en **`/etc/cluster/cluster.conf`**. Además, los recursos de hijo no-tipificado se inician después de que todos los recursos de hijo tipificado hayan iniciado y parado antes de que cualquier recurso de hijo tipificado haya parado.

Nota

El único recurso para implementar una solicitud definida *tipo de recurso hijo* es el recurso de servicio.

Para obtener mayor información sobre solicitud de inicio y parada del recurso de hijo tipificado, consulte la Sección C.2.1, “Solicitud de inicio y parada de recursos de hijo tipificado”. Asimismo, para obtener información sobre solicitud de inicio y parada de recursos de hijo no-tipificado, consulte la Sección C.2.2, “Solicitud de inicio y parada de los recursos de hijo no-tipificado ”.

C.2.1. Solicitud de inicio y parada de recursos de hijo tipificado

Para un recurso de hijo tipificado, el atributo de tipo para un recurso de hijo define el orden de inicio y parada de cada tipo de recurso con un número de 1 a 100; un valor para iniciar y un valor para detenerse. Entre más bajo sea el tipo de recurso, más temprano el tipo de recurso inicia o se detiene. Por ejemplo, la Tabla C.1, “Tipo de recursos de hijos y orden de parada” muestra los valores de inicio y parada para cada tipo de recurso; el Ejemplo C.2, “Iniciar recursos y detener valores: Extracto del Agente de recursos de servicio, **`service.sh`**” muestra los valores de inicio y parada tal y como aparecen en el Agente de recursos de servicio, **`service.sh`**. Para el Recurso de servicios, todos los hijos de LVM se inician primero seguidos de todos los hijos del sistema de archivos, seguidos por todos los hijos de script y así sucesivamente.

Tabla C.1. Tipo de recursos de hijos y orden de parada

Recursos	Tipo de hijo	Valor de orden de inicio	Valor de orden de parada
LVM	lvm	1	9
Sistema de archivos	fs	2	8
Sistema de archivos GFS2	clusterfs	3	7
NFS Mount	netfs	4	6
NFS Export	nfsexport	5	5
Cliente NFS	nfsclient	6	4
Dirección IP	ip	7	2
Samba	smb	8	3
Script	script	9	1

Ejemplo C.2. Iniciar recursos y detener valores: Extracto del Agente de recursos de servicio, `service.sh`

```
<special tag="rgmanager">
    <attributes root="1" maxinstances="1"/>
    <child type="lvm" start="1" stop="9"/>
    <child type="fs" start="2" stop="8"/>
    <child type="clusterfs" start="3" stop="7"/>
    <child type="netfs" start="4" stop="6"/>
    <child type="nfsexport" start="5" stop="5"/>
    <child type="nfsclient" start="6" stop="4"/>
    <child type="ip" start="7" stop="2"/>
    <child type="smb" start="8" stop="3"/>
    <child type="script" start="9" stop="1"/>
</special>
```

El orden dentro de un tipo de recursos se preserva tal como está en el archivo de configuración de clúster, **`/etc/cluster/cluster.conf`**. Por ejemplo, considere el orden de inicio y el orden de parada de los recursos de hijo tipificado en el Ejemplo C.3, “Solicitud dentro de un tipo de recursos”.

Ejemplo C.3. Solicitud dentro de un tipo de recursos

```
<service name="foo">
  <script name="1" .../>
  <lvm name="1" .../>
  <ip address="10.1.1.1" .../>
  <fs name="1" .../>
  <lvm name="2" .../>
</service>
```

Orden de inicio de recursos de hijo tipificado

En el Ejemplo C.3, “Solicitud dentro de un tipo de recursos”, los recursos se inician en el siguiente orden:

1. **`lvm:1`** — Es un recurso LVM. Todos los recursos LVM se inician primero. **`lvm:1`** (**`<lvm name="1" .../>`**) es el primer recurso LVM iniciado entre recursos LVM porque es el primer recurso LVM listado en la porción del servicio *foo* de **`/etc/cluster/cluster.conf`**.
2. **`lvm:2`** — Este es un recurso LVM. Todos los recursos LVM se inician primero. **`lvm:2`** (**`<lvm`**

name="2" .../>) se inicia después de **lvm:1** porque está listado después de **lvm:1** en la porción de servicio *foo* de **/etc/cluster/cluster.conf**.

3. **fs:1** — Este es un recurso de sistema de archivos. Si hubiera otros recursos de sistema de archivos en Servicio *foo*, iniciarían en el orden listado en la porción del Servicio *foo* de **/etc/cluster/cluster.conf**.
4. **ip:10.1.1.1** — Este es un recurso de dirección IP. Si hubiera otros recursos de dirección IP en el Servicio *foo*, iniciarían en el orden listado en la porción del Servicio *foo* de **/etc/cluster/cluster.conf**.
5. **script:1** — Este es un recurso de script. Si hubiera otros recursos de script en el Servicio *foo*, iniciarían en el orden listado en la porción del Servicio *foo* de **/etc/cluster/cluster.conf**.

Orden de parada de recurso de hijo tipificado

En el Ejemplo C.3, "Solicitud dentro de un tipo de recursos", los recursos se detienen en el siguiente orden:

1. **script:1** — Este es un recurso de script. Si hubiera otros recursos de Script en el Servicio *foo*, se detendrían en orden inverso listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.
2. **ip:10.1.1.1** — Este es un recurso de dirección IP. Si hubiera otros recursos de dirección IP en Servicio *foo*, se detendrían en el orden inverso listado en la porción del Servicio *foo* de **/etc/cluster/cluster.conf**.
3. **fs:1** — Este es un recurso de sistema de archivos. Si hubiera otros recursos de sistemas de archivos en el servicio *foo*, se detendrían en el orden inverso listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.
4. **lvm:2** — Este es un recurso LVM. Todos los recursos LVM se detienen de último. **lvm:2** (**<lvm name="2" .../>**) se detiene antes de **lvm:1**; los recursos dentro de un grupo de tipo de recursos se detienen en el orden inverso listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.
5. **lvm:1** — Este es un recurso LVM. Todos los recursos LVM se detienen de último. **lvm:1** (**<lvm name="1" .../>**) se detiene después de **lvm:2**; los recursos dentro de un grupo de un tipo de recursos se detienen en el orden inverso listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.

C.2.2. Solicitud de inicio y parada de los recursos de hijo no-tipificado

Se requieren consideraciones adicionales para los recursos hijos no tipificados. Para los recursos hijos no tipificados, el recurso de servicios no especifica de forma explícita el orden de inicio y de parada. En su lugar, el orden de inicio y de parada se determinan según el orden del recurso hijo en **/etc/cluster/cluster.conf**. Además, los recursos hijos no tipificados se inician después de que todos los recursos hijo y se detienen, antes de cualquier recurso tipificado.

Por ejemplo, considere el orden de inicio y parada de recursos de hijo no-tipificados en el Ejemplo C.4, "Recursos de hijo no tipificado y recursos de hijo tipificado en un servicio".

Ejemplo C.4. Recursos de hijo no tipificado y recursos de hijo tipificado en un servicio

```
<service name="foo">
  <script name="1" .../>
  <nontypedresource name="foo"/>
  <lvm name="1" .../>
  <nontypedresourcetwo name="bar"/>
  <ip address="10.1.1.1" .../>
  <fs name="1" .../>
  <lvm name="2" .../>
</service>
```

Orden de inicio de recursos de hijo no tipificado

En el Ejemplo C.4, "Recursos de hijo no tipificado y recursos de hijo tipificado en un servicio", los recursos de hijo se inician en el siguiente orden:

1. **lvm:1** — Es un recurso LVM. Todos los recursos LVM se inician primero. **lvm:1** (**<lvm name="1" .../>**) es el primer recurso LVM iniciado entre recursos LVM porque es el primer recurso LVM listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.
2. **lvm:2** — Este es un recurso LVM. Todos los recursos LVM se inician primero. **lvm:2** (**<lvm**

name="2" .../>) se inicia después de **lvm:1** porque está listado después de **lvm:1** en la porción de servicio *foo* de **/etc/cluster/cluster.conf**.

3. **fs:1** — Este es un recurso de sistema de archivos. Si hubiera otros recursos de sistema de archivos en Servicio *foo*, iniciarían en el orden listado en la porción del Servicio *foo* de **/etc/cluster/cluster.conf**.
4. **ip:10.1.1.1** — Este es un recurso de dirección IP. Si hubiera otros recursos de dirección IP en el Servicio *foo*, iniciarían en el orden listado en la porción del Servicio *foo* de **/etc/cluster/cluster.conf**.
5. **script:1** — Este es un recurso de script. Si hubiera otros recursos de script en el Servicio *foo*, iniciarían en el orden listado en la porción del Servicio *foo* de **/etc/cluster/cluster.conf**.
6. **nontypedresource:foo** — Este es un recurso no tipificado. Debido a que es un recurso no tipificado, se inicia después de que los recursos tipificados inicien. Además, el orden en el recurso de servicio es anterior al otro recurso no tipificado, **nontypedresourcetwo:bar**; por lo tanto, se inicia antes de **nontypedresourcetwo:bar**. (Los recursos no tipificados se inician en orden en que aparecen en el recurso de servicio).
7. **nontypedresourcetwo:bar** — Este es un recurso no-tipificado. Puesto que es un recurso no-tipificado, se inicia después de iniciar recursos tipificados. Además, el orden en el recurso de Servicio es posterior a otro recurso no-tipificado, **nontypedresource:foo**; por lo tanto, se inicia después de **nontypedresource:foo**. (Los recursos no-tipificados se inician en el orden que aparecen en el recurso de Servicio).

Orden de parada de recursos no-tipificados

En el Ejemplo C.4, “Recursos de hijo no tipificado y recursos de hijo tipificado en un servicio”, los recursos de hijo se detienen en el siguiente orden:

1. **nontypedresourcetwo:bar** — Este es un recurso no tipificado. Puesto que es un recurso no-tipificado, se detiene antes de los recursos tipificados. Además, el orden en el recurso de Servicio es posterior al otro recurso no tipificado, **nontypedresource:foo**; por lo tanto, se detiene antes de **nontypedresource:foo**. (Los recursos no tipificados se detienen en el orden inverso al que aparecen en el recurso de servicio).
2. **nontypedresource:foo** — Este no es un recurso tipificado. Puesto que no lo es, se detendrá antes de que los recursos tipificados se detengan. Además, su orden en el recurso de servicios va delante del otro recurso no tipificado , **nontypedresourcetwo:bar**; por lo tanto, se detendrá después de **nontypedresourcetwo:bar**. (Los recursos no tipificados se detienen en orden inverso al que aparecen en el recurso de servicios).
3. **script:1** — Este es un recurso de script. Si hubiera otros recursos de Script en el Servicio *foo*, se detendrían en orden inverso listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.
4. **ip:10.1.1.1** — Este es un recurso de dirección IP. Si hubiera otros recursos de dirección IP en Servicio *foo*, se detendrían en el orden inverso listado en la porción del Servicio *foo* de **/etc/cluster/cluster.conf**.
5. **fs:1** — Este es un recurso de sistema de archivos. Si hubiera otros recursos de sistemas de archivos en el servicio *foo*, se detendrían en el orden inverso listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.
6. **lvm:2** — Este es un recurso LVM. Todos los recursos LVM se detienen de último. **lvm:2** (**<lvm name="2" .../>**) se detiene antes de **lvm:1**; los recursos dentro de un grupo de tipo de recursos se detienen en el orden inverso listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.
7. **lvm:1** — Este es un recurso LVM. Todos los recursos LVM se detienen de último. **lvm:1** (**<lvm name="1" .../>**) se detiene después de **lvm:2**; los recursos dentro de un grupo de un tipo de recursos se detienen en el orden inverso listado en la porción del servicio *foo* de **/etc/cluster/cluster.conf**.

C.3. Herencia, los "recursos" Bloques y reutilización de recursos

Algunos recursos se benefician al heredar valores de un recurso de padre; es decir comúnmente el caso en un servicio NFS. El Ejemplo C.5, “Configuración de servicio NFS para reutilización y herencia” muestra una configuración de servicio NFS típica, establecida para reutilización de recurso y herencia.

Ejemplo C.5. Configuración de servicio NFS para reutilización y herencia

```
    <resources>
        <nfsclient name="bob" target="bob.example.com"
options="rw,no_root_squash"/>
        <nfsclient name="jim" target="jim.example.com"
options="rw,no_root_squash"/>
        <nfsexport name="exports"/>
    </resources>
    <service name="foo">
        <fs name="1" mountpoint="/mnt/foo" device="/dev/sdb1" fsid="12344">
            <nfsexport ref="exports">  <!-- nfsexport's path and fsid
attributes
                                           are inherited from the mountpoint
&
                                           fsid attribute of the parent fs
                                           resource -->
                <nfsclient ref="bob"/> <!-- nfsclient's path is inherited
from the
                                           mountpoint and the fsid is added
to the
                                           options string during export -->
                <nfsclient ref="jim"/>
            </nfsexport>
        </fs>
        <fs name="2" mountpoint="/mnt/bar" device="/dev/sdb2" fsid="12345">
            <nfsexport ref="exports">
                <nfsclient ref="bob"/> <!-- Because all of the critical data
for this
                                           resource is either defined in
the
                                           resources block or inherited, we
can
                                           reference it again! -->
                <nfsclient ref="jim"/>
            </nfsexport>
        </fs>
        <ip address="10.2.13.20"/>
    </service>
```

Si el servicio fuera plano (es decir, sin relaciones padre/hijo), se necesitaría configurarlo así:

- El servicio necesitaría cuatro recursos nfsclient — uno por sistema de archivos (un total de dos para sistemas de archivos), y uno por máquina de destino (un total de dos para máquinas de destino).
- El servicio necesitaría especificar la ruta de exportación y el ID del sistema de archivos para cada nfsclient, el cual introduce posibilidades de errores en la configuración.

Sin embargo, en el Ejemplo C.5, “Configuración de servicio NFS para reutilización y herencia” los recursos de cliente NFS *nfsclient:bob* y *nfsclient:jim* se definen una sola vez; igualmente, el recurso de exportación NFS *nfsexport:exports* se define una sola vez. Todos los atributos requeridos por los recursos se heredan de recursos padres. Ya que los atributos heredados son dinámicos (y no entran en conflicto con ningún otro), es posible reutilizar esos recursos — los cuales están definidos en el bloque de recursos. No es práctico configurar algunos recursos en varios sitios. Por ejemplo, si configura un recurso de sistema de archivos en varios sitios puede ocasionar problemas, puesto que puede resultar montando un sistema de archivos en dos nodos.

C.4. Recuperación de fallas y subárboles independientes

En la mayoría de entornos empresariales, el curso de acción normal para recuperación de un servicio es reiniciar todo el servicio si cualquier componente en el servicio falla. Por ejemplo, en el Ejemplo C.6, “Recuperación de fallas normal del Servicio *foo*”, si alguno de los scripts definidos en este servicio falla, el curso normal de la acción es reiniciar (reubicar o desactivar, de acuerdo con la política de recuperación del servicio) el servicio. No obstante, en algunas circunstancias, algunas partes de un servicio pueden considerarse como no-críticas; y puede ser necesario solamente

reiniciar una parte del servicio, antes de intentar la recuperación normal. Para lograrlo, puede usar el atributo ***__independent_subtree***. Por ejemplo, en el Ejemplo C.7, "Recuperación de fallas del servicio *foo* con el atributo ***__independent_subtree***", el atributo ***__independent_subtree*** sirve para:

- Si script:script_one falla, reinicie script:script_one, script:script_two, y script:script_three.
- Si script:script_two falla, reinicie solamente script:script_two.
- Si script:script_three falla, reinicie script:script_one, script:script_two, y script:script_three.
- Si script:script_four falla, reinicie todo el servicio total.

Ejemplo C.6. Recuperación de fallas normal del Servicio *foo*

```
<service name="foo">
      <script name="script_one" ...>
          <script name="script_two" .../>
      </script>
      <script name="script_three" .../>
</service>
```

Ejemplo C.7. Recuperación de fallas del servicio *foo* con el atributo *__independent_subtree*

```
<service name="foo">
      <script name="script_one" __independent_subtree="1" ...>
          <script name="script_two" __independent_subtree="1" .../>
          <script name="script_three" .../>
      </script>
      <script name="script_four" .../>
</service>
```

En algunas circunstancias, si el componente de un servicio falla, usted podrá desactivar solamente ese componente sin necesidad de desactivar todo el servicio, para evitar que los otros servicios afecten el uso de otros componentes de ese servicio. A partir del lanzamiento de Red Hat Enterprise Linux 6.1, puede llevar a cabo esto con el atributo ***__independent_subtree="2"***, el cual designa el subárbol independiente como no crítico.

Nota

Puede usar el indicador no-crítico en recursos de referencias únicas. El indicador no crítico funciona con todos los recursos a todos los niveles del árbol de recursos, pero no debe usarse en el nivel superior en la definición de servicios o máquinas virtuales.

A partir del lanzamiento de Red Hat Enterprise Linux 6.1, usted puede establecer el reinicio máximo y reiniciar expiraciones por nodo en el árbol independiente de recursos de subárboles. Para establecer estos umbrales, puede usar los siguientes atributos:

- **__max_restarts** configura el número máximo de reinicios tolerados antes de ceder.
- **__restart_expire_time** configura la cantidad de tiempo, en segundos, después del cual ya no se intenta reiniciar.

C.5. Depuración y prueba de servicios y ordenamiento de recursos

Puede depurar y probar servicios y solicitud de recursos con la herramienta **rg_test**. **rg_test** es una herramienta de línea de comandos proporcionada por el paquete **rgmanager** que se ejecuta desde un shell o una terminal (no está disponible en **Conga**). La Tabla C.2, "Resumen de herramientas **rg_test**" resume las acciones y sintaxis para la herramienta **rg_test**.

Tabla C.2. Resumen de herramientas `rg_test`

Acción	Sintaxis
Mostrar las reglas de recursos que entiende `rg_test`.	`rg_test rules`
Probar una configuración (y /usr/share/cluster) por si hay errores o agentes de recursos redundantes.	`rg_test test /etc/cluster/cluster.conf`
Mostrar la solicitud de inicio y parada de un servicio.	Mostrar el orden de inicio: `rg_test noop /etc/cluster/cluster.conf start service` ***`servicename`*** Mostrar el orden de parada: `rg_test noop /etc/cluster/cluster.conf stop service` ***`servicename`***
Iniciar o parar explícitamente un servicio.	**Importante** Solamente haga esto en un nodo, y siempre desactive primero el servicio en rgmanager. Iniciar un servicio: `rg_test test /etc/cluster/cluster.conf start service` ***`servicename`*** Parar el servicio: `rg_test test /etc/cluster/cluster.conf stop service` ***`servicename`***
Calcular y mostrar el árbol de recursos delta entre dos archivos cluster.conf.	`rg_test delta` ***`cluster.conf file 1 cluster.conf file 2`*** Por ejemplo: `rg_test delta /etc/cluster/cluster.conf.bak /etc/cluster/cluster.conf`

Revisión de recursos de servicios de clúster y tiempo de espera de conmutación

Este apéndice describe la forma como **rgmanager** monitoriza el estatus de los recursos de clúster y describe cómo modificar el intervalo de revisión de estatus. El apéndice también describe el parámetro de servicio **__enforce_timeouts** indicando que el tiempo de espera para una operación puede hacer que el servicio falle.

Nota

Para comprender totalmente la información en este apéndice, deberá conocer en detalle los agentes de recursos y el archivo de configuración de clúster **/etc/cluster/cluster.conf**. Para obtener una lista completa y descripción de los elementos de **cluster.conf** y atributos, consulte el esquema de clúster en **/usr/share/cluster/cluster.rng**, y el esquema anotado en **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (por ejemplo, **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

D.1. Cómo modificar el intervalo de revisión de estatus de recursos

rgmanager revisa el estatus de recursos individuales, no de todos los servicios. Cada 10 segundos, rgmanager escanea el árbol de recursos, buscando recursos que han pasado su intervalo de "revisión de estatus".

Cada agente de recursos especifica la cantidad de tiempo entre revisiones de estatus periódicas. Cada recurso utiliza dichos valores a menos que se sobrescriban de forma explícita en el archivo **cluster.conf** con la etiqueta especial **<action>**:

```
<action name="status" depth="*" interval="10" />
```

Esta etiqueta es un hijo de recursos especial en el archivo **cluster.conf**. Por ejemplo, si tuviera un recurso de sistema de archivos para el cual desea sobrescribir el intervalo de revisión de estatus, podría especificar el recurso de sistema de archivos en el archivo **cluster.conf** así:

```
<fs name="test" device="/dev/sdb3">
  <action name="status" depth="*" interval="10" />
  <nfsexport...>
  </nfsexport>
</fs>
```

Algunos agentes ofrecen múltiples "profundidades" de revisión. Por ejemplo, una revisión de estatus de sistema de archivos (profundidad 0) revisa si el sistema de archivos está montado en el sitio correcto. Una profundidad más intensa es 10, la cual revisa si usted puede leer un archivo desde el sistema de archivos. La revisión de estatus de profundidad 20 revisa si usted puede escribir al sistema de archivos. En el ejemplo que damos aquí, la **depth** (profundidad) se establece a *, lo cual indica que dichos valores deben utilizarse para todas las profundidades. El resultado es que el sistema de archivos **test** se revisa a una profundidad superior definida por el agente de recursos (en este caso, 20) cada 10 segundos.

D.2. Aplicación de tiempos de espera en recursos

No hay tiempo de espera para iniciar, detener o conmutar recursos. Algunos recursos se tardan una cantidad de tiempo indeterminada para iniciar o detenerse. Infortunadamente, el no poder detenerse (incluyendo tiempo de espera) hace que el servicio no funcione (estado fallido). Si desea activar la aplicación de tiempo de espera en cada recurso en un servicio individual, puede añadir **__enforce_timeouts="1"** a la referencia en el archivo **cluster.conf**.

El siguiente ejemplo muestra un servicio de clúster configurado con el atributo **__enforce_timeouts** establecido para el recurso **netfs**. Si con este atributo establecido, se tarda más de 30 segundos en desmontar el sistema de archivos NFS durante la recuperación, la operación expirará haciendo que el servicio entre al estado fallido.

```
</screen>
<rm>
  <failoverdomains/>
  <resources>
    <netfs export="/nfstest" force_unmount="1" fstype="nfs" host="10.65.48.65"
           mountpoint="/data/nfstest" name="nfstest_data"
options="rw,sync,soft"/>
  </resources>
  <service autostart="1" exclusive="0" name="nfs_client_test"
recovery="relocate">
    <netfs ref="nfstest_data" __enforce_timeouts="1"/>
  </service>
</rm>
```

Resumen de herramientas de línea de comandos

Tabla E.1, "Resumen de herramientas de líneas de comandos" resume las herramientas preferidas de líneas de comandos para configurar y administrar adiciones de alta disponibilidad. Para obtener mayor información sobre comandos y variables, consulte la página de manual para cada herramienta de línea de comandos.

Tabla E.1. Resumen de herramientas de líneas de comandos

Herramientas de línea de comandos	Utilizadas con	Propósito
ccs_config_dump — Herramienta de vaciado de configuración de clúster	Infraestructura de clúster	**ccs_config_dump** genera salida XML de configuración en ejecución. La configuración en ejecución es algunas veces diferente a la configuración almacenada en el archivo de configuración, ya que algunos subsistemas almacenan o establecen información predeterminada en la configuración. Dichos valores suelen estar presentes en una versión en disco de la configuración, pero se requieren en el momento de ejecución para que el clúster funcione correctamente. Para obtener mayor información sobre esta herramienta, consulte la página de manual (8) ccs_config_dump.
ccs_config_validate — Herramienta de validación de configuración de clúster	Infraestructura de clúster	**ccs_config_validate** valida a **cluster.conf** con el esquema, **cluster.rng** (localizado en **/usr/share/cluster/cluster.rng** en cada nodo). Para obtener mayor información sobre esta herramienta, consulte la página de manual (8) ccs_config_validate.
clustat — Herramienta de estatus de clúster	Componentes de administración de servicios de alta disponibilidad	El comando **clustat** muestra el estatus del clúster. Muestra información de membresía, vista de cuórum y estado de todos los servicios de usuario configurados. Para obtener mayor información sobre esta herramienta, consulte la página de manual (8) clustat.
clusvcadm — Herramienta de administración de servicios de usuario de clúster	Componentes de administración de servicios de alta disponibilidad	El comando **clusvcadm** le permite habilitar, inhabilitar, reubicar, y reiniciar servicios de alta disponibilidad en un clúster. Para obtener mayor información sobre esta herramienta, consulte la página de manual (8) clusvcadm.
cman_tool — Herramienta de administración de clúster	Infraestructura de clúster	**cman_tool** es un programa que maneja el gestor de clúster CMAN. Permite conectar a un clúster, abandonar a un clúster, matar a un nodo, o cambiar los votos de cuórum esperados de un nodo en un clúster. Para obtener mayor información sobre esta herramienta, consulte la página de manual (8) cman_tool.
fence_tool — Herramienta de valla	Infraestructura de clúster	**fence_tool** es un programa que sirve para conectar o abandonar el dominio de valla. Para obtener mayor información sobre esta herramienta, consulte la página de manual (8) fence_tool.

Alta disponibilidad de LVM (HA-LVM)

La adición de alta disponibilidad de Red Hat ofrece soporte para volúmenes LVM de alta disponibilidad (HA-LVM) en una configuración de conmutación. Esto es diferente a las configuraciones active/active activadas por el Gestor de volúmen lógico en clúster (CLVM), el cual es un conjunto de extensiones de agrupamiento para LVM que permiten que un clúster de computadores administre el almacenaje compartido.

Cuando utilice CLVM o HA-LVM debe basarse en las necesidades de aplicaciones o servicios que se emplean.

- Si las aplicaciones reconocen a los clústeres y han sido ajustados para que se ejecuten de forma simultánea en múltiples máquinas, entonces se debe utilizar CLVM. Específicamente, si más de un nodo de su clúster requiere acceso a su almacenaje que luego se comparte entre los nodos activos, entonces debe usar CLVM. CLVM permite al usuario configurar volúmenes lógicos en almacenaje compartido al bloquear el acceso al almacenaje físico mientras un volumen lógico está siendo configurado, y utiliza servicios de bloqueo en clúster para manejar el almacenaje compartido. Para obtener información sobre CLVM y configuración de LVM en general, consulte *Administración del gestor de volumen lógico*.
- Si las aplicaciones se ejecutan de forma óptima en configuraciones activa/pasiva (conmutación) donde solo un nodo individual que accede al almacenaje está activo en cualquier momento, debe usar agentes de adminitración de volúmenes lógicos de alta disponibilidad (HA-LVM).

La mayoría de las aplicaciones se ejecutarán en una configuración activa/pasiva, ya que no están diseñadas u optimizadas para ejecutarse simultáneamente con otras instancias. Si elige ejecutar una aplicación que no reconozca los clústeres en volúmenes lógicos el rendimiento podría degradarse si el volumen lógico ha sido copiado en espejo. Esto se debe a que hay una sobrecarga de comunicación de clúster para los volúmenes lógicos en dichas instancias. Una aplicación que reconozca los clústeres, debe ser capaz de lograr mejoras en rendimiento por encima de las pérdidas en rendimiento introducidas por los sistemas de archivos de clúster y los volúmenes lógicos que con reconozcan clústeres. Esto es factible para algunas aplicaciones y cargas de trabajo y más fácil para otras. El determinar cuáles son los requerimientos del clúster y si el esfuerzo adicional para mejorar un clúster activo/activo, rinde beneficios, es el camino para elegir entre las dos variantes de LVM. La mayoría de los usuarios lograrán los mejores resultados de alta disponibilidad al usar HA-LVM.

HA-LVM y CLVM son similares en el hecho de que pueden evitar la corrupción de los metadatos de LVM y sus volúmenes lógicos, la cual podría presentarse si múltiples máquinas pudieran hacer cambios de sobreposición. HA-LVM impone la restricción de que un volumen lógico solo puede estar activado exclusivamente; es decir, activo en una sola máquina a la vez. Esto significa que solo se usan las implementaciones (no clúster) de controladores de almacenaje. Al evitar así la sobrecarga de coordinación de clúster, aumenta el rendimiento. CLVM no impone estas restricciones - el usuario es libre de activar un volumen lógico en todas las máquinas en un clúster; esto fuerza el uso de controladores de almacenaje de clúster que permiten que sistemas de archivos con reconocimiento de clúster y aplicaciones se coloquen en la parte superior.

HA-LVM puede configurar el uso de uno de los dos métodos para lograr su mandato de activación de volumen lógico exclusivo.

- El método preferido usa CLVM, pero solo activará volúmenes lógicos de forma exclusiva. Esto tiene la ventaja de una configuración más fácil y de una mejor prevención de errores administrativos (tales como retirar un volumen lógico que no esté en uso). Para usar CLVM, el software de adición de alta disponibilidad y el software de adición de almacenaje resistente, incluyendo el demonio **`clvmd`**, deben estar en ejecución.

  El procedimiento para configurar HA-LVM mediante este método se describe en la Sección F.1, “Configuración de conmutación de HA-LVM con CLVM (preferido) ”.
- El segundo método usa el bloqueo de máquina local y las etiquetas o "tags" LVM. Este método tiene la ventaja de que no se requiere ningún paquete de clúster LVM; sin embargo, hay más pasos en la configuración y no previene al administrador de retirar un volumen lógico de un nodo erradamente en el clúster donde no esté activo. El procedimiento para configurar HA-LVM con este método se describe en la Sección F.2, “Configuración de conmutación HA-LVM con etiquetas”.

F.1. Configuración de conmutación de HA-LVM con CLVM (preferido)

Para configurar conmutación de HA-LVM (con la variante preferida CLVM), realice los siguientes pasos:

1. Asegúrese de que su sistema esté configurado para soportar CLVM, el cual requiere lo

siguiente:

- La adición de alta disponibilidad y la adición de almacenaje resistente instalados, incluyendo el paquete **cmirror** si los volúmenes lógicos de CLVM deben ser copiados en espejo.
- El parámetro **locking_type** en la sección global del archivo **/etc/lvm/lvm.conf** se establece al valor de '3'.
- El software de adición de alta disponibilidad y de adición de almacenaje resistente, incluyendo el demonio **clvmd**, deben estar en ejecución. Para copia en espejo de CLVM, también se debe iniciar el servicio **cmirrord**.

2. Cree el volumen lógico y el sistema de archivos mediante LVM estándar y los comandos de sistema de archivo, como en el siguiente ejemplo:

```
# pvcreate /dev/sd[cde]1

# vgcreate -cy shared_vg /dev/sd[cde]1

# lvcreate -L 10G -n ha_lv shared_vg

# mkfs.ext4 /dev/shared_vg/ha_lv

# lvchange -an shared_vg/ha_lv
```

Para obtener información sobre creación de volúmenes lógicos LVM, consulte *Administración del gestor de volumen lógico*.

3. Edite el archivo **/etc/cluster/cluster.conf** para incluir el volumen recién creado como un recurso en uno de sus servicios. También puede usar **Conga** o el comando **ccs** para configurar LVM y los recursos del sistema de archivos para el clúster. La siguiente es una muestra de la sección del gestor de recursos del archivo **/etc/cluster/cluster.conf** que configura un volumen lógico CLVM como recurso de clúster:

```
<rm>
   <failoverdomains>
       <failoverdomain name="FD" ordered="1" restricted="0">
          <failoverdomainnode name="neo-01" priority="1"/>
          <failoverdomainnode name="neo-02" priority="2"/>
       </failoverdomain>
   </failoverdomains>
   <resources>
       <lvm name="lvm" vg_name="shared_vg" lv_name="ha-lv"/>
       <fs name="FS" device="/dev/shared_vg/ha-lv" force_fsck="0"
force_unmount="1" fsid="64050" fstype="ext4" mountpoint="/mnt" options=""
self_fence="0"/>
   </resources>
   <service autostart="1" domain="FD" name="serv" recovery="relocate">
       <lvm ref="lvm"/>
       <fs ref="FS"/>
   </service>
</rm>
```

F.2. Configuración de conmutación HA-LVM con etiquetas

Para configurar la conmutación de HA-LVM con etiquetas en el archivo **/etc/lvm/lvm.conf**, realice los siguientes pasos:

1. Asegúrese que el parámetro **locking_type** en la sección global del archivo **/etc/lvm/lvm.conf** se establezca al valor de '1'.
2. Cree el volumen lógico y el sistema de archivos mediante LVM estándar y los comandos de sistema de archivo, como en el siguiente ejemplo:

```
# pvcreate /dev/sd[cde]1

# vgcreate shared_vg /dev/sd[cde]1

# lvcreate -L 10G -n ha_lv shared_vg

# mkfs.ext4 /dev/shared_vg/ha_lv
```

Para obtener información sobre creación de volúmenes lógicos LVM, consulte *Administración del gestor de volumen lógico*.

3. Edite el archivo **/etc/cluster/cluster.conf** para incluir el volumen recién creado como un recurso en uno de sus servicios. También puede usar **Conga** o el comando **ccs** para configurar LVM y los recursos del sistema de archivos para el clúster. La siguiente es una muestra de la sección del gestor de recursos del archivo **/etc/cluster/cluster.conf** que configura un volumen lógico CLVM como recurso de clúster:

```
<rm>
   <failoverdomains>
       <failoverdomain name="FD" ordered="1" restricted="0">
          <failoverdomainnode name="neo-01" priority="1"/>
          <failoverdomainnode name="neo-02" priority="2"/>
       </failoverdomain>
   </failoverdomains>
   <resources>
       <lvm name="lvm" vg_name="shared_vg" lv_name="ha_lv"/>
       <fs name="FS" device="/dev/shared_vg/ha_lv" force_fsck="0"
force_unmount="1" fsid="64050" fstype="ext4" mountpoint="/mnt" options=""
self_fence="0"/>
   </resources>
   <service autostart="1" domain="FD" name="serv" recovery="relocate">
       <lvm ref="lvm"/>
       <fs ref="FS"/>
   </service>
</rm>
```

Nota

Si hay múltiples volúmenes lógicos en el grupo de volumen, entonces el nombre del volumen lógico (**lv_name**) en el recurso **lvm** se debe dejar en blanco o sin especificar. Observe también que en la configuración de HA-LVM, un grupo de volumen puede ser utilizado por un servicio individual único.

4. Edite el campo **volume_list** en el archivo **/etc/lvm/lvm.conf**. Incluya el nombre de su grupo de volumen raíz y su nombre de host como aparece en el archivo **/etc/cluster/cluster.conf** precedido por **@**. El nombre de host a incluir aquí es la máquina en la cual esta modificando el archivo **lvm.conf**, no ningún nombre de host remoto. Observe que esta cadena *DEBE* coincidir con el nombre de nodo determinado en el archivo **cluster.conf**. A continuación, una muestra de la entrada del archvo **/etc/lvm/lvm.conf**:

```
volume_list = [ "VolGroup00", "@neo-01" ]
```

Esta etiqueta se utilizará para activar los LV y VG compartidos. *NO* incluye los nombres de ningún grupo de volumen que haya sido compartido mediante HA-LVM.

5. Actualizar el dispositivo **initrd** en todos sus nodos de clúster:

```
# dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

6. Reinicie todos los nodos para verificar si se está utilizando el dispositivo correcto de **initrd**.

Historial de revisiones

Revisión 5.0-25.2 **Tue Apr 30 2013** **Gladys Guerrero-Lozano**
traducción completa

Revisión 5.0-25.1 **Thu Apr 18 2013** **Chester Cheng**
Los archivos de traducción sincronizados con fuentes XML 5.0-25

Revisión 5.0-25 **Mon Feb 18 2013** **Steven Levine**
Versión para lanzamiento de disponibilidad general 6.4

Revisión 5.0-23 **Wed Jan 30 2013** **Steven Levine**
Resuelve: 901641
Corrige y aclara reglas Iptables.

Revisión 5.0-22 **Tue Jan 29 2013** **Steven Levine**
Resuelve: 788636
Documenta la configuración RRP mediante el comando **ccs**.

Resuelve: 789010
Documenta la configuración RRP en el archivo **cluster.conf**.

Revisión 5.0-20 **Fri Jan 18 2013** **Steven Levine**
Resuelve: 894097
Retira el consejo para garantizar usted utilice etiguetado VLAN.

Resuelve: 845365
Indica que los modos de enlace 0 y 2 ahora tienen soporte.

Revisión 5.0-19 **Thu Jan 17 2013** **Steven Levine**
Resuelve: 896234
Aclara la terminología de referencias del nodo de clúster.

Revisión 5.0-16 **Mon Nov 26 2012** **Steven Levine**
Versión para lanzamiento beta 6.4

Revisión 5.0-15 **Wed Nov 20 2012** **Steven Levine**
Resuelve: 838988
Documenta el atributo 'nfsrestart' para los agentes de recursos del sistema de archivos.

Resuelve: 843169
Documenta el agente de vallas IBM IPDU

Resuelve: 846121
Documenta el agente de vallas del controlador de red de energía Eaton (Interfaz SNMP).

Resuelve: 856834
Documenta el agente de vallas HP Bladesystem.

Resuelve: 865313
Documenta el agente de recursos del servidor NFS.

Resuelve: 862281
Aclara qué **ccs** sobrescriben los parámetros anteriores.

Resuelve: 846205
Documenta el filtraje de cortafuegos de **iptables** para el componente **igmp**.

Resuelve: 857172
Documenta la capacidad de retirar usuarios desde luci.

Resuelve: 857165
Documenta el parámetro de nivel de privilegios del agente de vallas IPMI.

Resuelve: 840912
Aclara el problema de formateo con la tabla de parámetros de recursos.

Resuelve: 849240,870292
Aclara el procedimiento de instalación.

Resuelve: 871165
Aclara la descripción del parámetro de dirección IP en la descripción del agente de recursos de dirección IP.

Resuelve: 845333, 869039, 856681
Corrige errores tipográficos y aclara ambigüedades técnicas.

Revisión 5.0-12 **Thu Nov 1 2012** **Steven Levine**
Se añadieron agentes de valla recién soportados.

Revisión 5.0-7 **Thu Oct 25 2012** **Steven Levine**
Se agregó una sección sobre semántica de sobrescritura.

Revisión 5.0-6 **Tue Oct 23 2012** **Steven Levine**
Se ha corregido el valor de Retraso posconexión.

Revisión 5.0-4 **Tue Oct 16 2012** **Steven Levine**
Se agregó descripción de recurso de servidor NFS.

Revisión 5.0-2 **Thu Oct 11 2012** **Steven Levine**
Actualizaciones a descripciones de Conga.

Revisión 5.0-1 **Mon Oct 8 2012** **Steven Levine**
Se aclara semántica de CCS

Revisión 4.0-5 **Fri Jun 15 2012** **Steven Levine**
Versión para lanzamiento G.A 6.3

Revisión 4.0-4 **Tue Jun 12 2012** **Steven Levine**
Resuelve: 830148
Garantiza consistencia de ejemplos de números de puerto para luci.

Revisión 4.0-3 **Tue May 21 2012** **Steven Levine**
Resuelve:696897
Añade información del parámetro cluster.conf a las tablas de parámetros de dispositivo de vallas y parámetros de recursos.

Resuelve: 811643
Añade procedimiento para restaurar una base de datos de **luci** en una máquina independiente..

Revisión 4.0-2 **Wed Apr 25 2012** **Steven Levine**
Resuelve: 815619
Retira la advertencia mediante unidifusion UDP con sistemas de archivos GFS2.

Revisión 4.0-1 **Fri Mar 30 2012** **Steven Levine**
Resuelve: 771447, 800069, 800061
Actualiza la documentación de **luci** para que sea consistente con la versión de Red Hat Enterprise Linux 6.3.

Resuelve: 712393
Añade información sobre capturar un núcleo de aplicación para RGManager.

Resuelve: 800074
Documenta el agente de recursos de `condor`.

Resuelve: 757904
Documenta la copia de seguridad de configuración de **luci** y la restauración.

Resuelve: 772374
Añade la sección sobre manejo de máquinas virtuales en un clúster.

Resuelve: 712378
Añade documentación para configurar HA-LVM.

Resuelve: 712400
Documenta opciones de depuración.

Resuelve: 751156
Documenta el nuevo parámetro **fence_ipmilan**.

Resuelve: 721373
Documenta los cambios de configuración que requieren un reinicio de clúster.

Revisión 3.0-5 **Thu Dec 1 2011** **Steven Levine**
Lanzamiento para GA de Red Hat Enterprise Linux 6.2

Resuelve: 755849
Corrige el ejemplo de parámetro monitor_link.

Revisión 3.0-4 **Mon Nov 7 2011** **Steven Levine**
Resuelve: 749857
Añade documentación para el dispositivo de valla RHEV-M REST API.

Revisión 3.0-3 **Fri Oct 21 2011** **Steven Levine**
Resuelve: #747181, #747182, #747184, #747185, #747186, #747187, #747188, #747189, #747190, #747192
Corrige los errores tipográficoa y ambiguedades encontradas durante la revisión de QE para Red Hat Enterprise Linux 6.2.

Revisión 3.0-2 **Fri Oct 7 2011** **Steven Levine**
Resuelve: #743757
Corrige la referencia al modo de enlace soportado en la sección de Detección y solución de errores.

Revisión 3.0-1 **Wed Sep 28 2011** **Steven Levine**
Revisión inicial para el lanzamiento Beta de Red Hat Enterprise Linux 6.2

Resuelve: #739613
Documenta soporte para que las nuevas opciones **ccs** muestren los dispositivos de vallas y los servicios disponibles..

Resuelve: #707740
Documenta actualizaciones para la interfaz de Conga y documenta soporte para permisos administrativos de usuario para Conga.

Resuelve: #731856
Documenta soporte para configurar **luci** mediante el archivo **/etc/sysconfig/luci**.

Resuelve: #736134
Documenta el soporte para transporte UDPU.

Resuelve: #736143
Documenta soporte para Samba en clúster.

Resuelve: #617634
Documenta cómo configurar la única dirección IP en la que se sirve **luci**.

Resuelve: #713259
Documenta soporte para el agente **fence_vmware_soap**.

Resuelve: #721009
Proporciona el enlace para el artículo 'Support Essentials'.

Resuelve: #717006
Proporciona información sobre el permiso de tráfico multidifusión a través del cortafuegos **iptables**.

Resuelve: #717008
Proporciona información sobre la revisión del servicio de clúster y el tiempo de conmutación.

Resuelve: #711868
Aclara la descripción de 'autostart'.

Resuelve: #728337
Documenta el procedimiento para añadir recursos **vm** con el comando **ccs**.

Resuelve: #725315, #733011, #733074, #733689
Corrige errores tipográficos.

Revisión 2.0-1 **Thu May 19 2011** **Steven Levine**
Revisión inicial para Red Hat Enterprise Linux 6.1

Resuelve: #671250
Documenta soporte para capturas SNMP.

Resuelve: #659753
Documenta el comando **ccs**.

Resuelve: #665055
Actualiza documentación de Conga para reflejar presentación actualizada y soporte de funcionalidades.

Resuelve: #680294
Documenta la necesidad de accceso de contraseña para el agente **ricci**.

Resuelve: #687871
Añade capítulo sobre detección y solución de errores.

Resuelve: #673217
Corrige errores tipográficos.

Resuelve: #675805
Añade referencia para esquema de **cluster.conf** para tablas de parámetros de recursos de alta disponibilidad.

Resuelve: #672697
Actualiza tablas de parámetros de dispositivos de valla que incluyen todos los dispositivos de vallas compatibles.

Resuelve: #677994
Corrige información para parámetros de agente de valla **fence_ilo**.

Resuelve: #629471
Añade nota técnica sobre valor de consenso de configuración en un clúster de dos nodos.

Resuelve: #579585
Actualiza la sección sobre actualización de software de adiciones de alta disponibilidad de Red Hat.

Resuelve: #643216
Aclara problemas menores a través del documento.

Resuelve: #643191
Proporciona mejoras y correcciones para la documentación de **luci** .

Resuelve: #704539
Actualiza la tabla de parámetros de recursos de Máquina virtual.

Revisión 1.0-1 **Wed Nov 10 2010** **Paul Kennedy**
Lanzamiento inicial para Red Hat Enterprise Linux 6

Índice

A

ACPI

- configuración, Cómo configurar ACPI para usar con dispositivos de valla integrados

Activación, tráfico multidifusión, Cómo configurar el cortafuegos de iptables para permitir

componentes de clúster

Administración de clúster, Antes de configurar la adición de alta disponibilidad de Red Hat, Administración de adición de alta disponibilidad de Red Hat con Conga, Administración de adición de alta disponibilidad de Red Hat con ccs, Administración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos

- abandono de un clúster, Hacer que un nodo abandone o se una a un clúster, Hacer que un nodo abandone o se una a un clúster

- actualización de configuración, Cómo actualizar una configuración

- actualización de una configuración de clúster mediante cman_tool version -r, Cómo actualizar una configuración con cman_tool version -r

- actualización de una configuración de clúster mediante scp, Actualizar y configurar mediante scp

- adición de nodo de clúster, Añadir un miembro a un clúster en ejecución, Añadir un miembro a un clúster en ejecución

- Administrar nodos de clúster, Administrar nodos de clúster, Administrar nodos de clúster

- borrado de un nodo desde la configuración; adición de un nodo a la configuración, Borrar o añadir un nodo

- borrar un clúster, Iniciar, parar, reiniciar, y borrar clústeres

- cómo mostrar servicios de alta disponibilidad con clustat, Cómo desplegar el estatus de servicio de alta disponibilidad con clustat

- consideraciones para usar disco de cuórum, Consideraciones para usar disco de cuórum

- consideraciones para usar qdisk, Consideraciones para usar disco de cuórum

- diagnóstico y corrección de problemas en un clúster, Cómo diagnosticar y corregir problemas en un clúster, Cómo diagnosticar y corregir problemas en un clúster

- eliminación de nodo de clúster, Borrado de un miembro de un clúster

- iniciar, parar, reiniciar un clúster, Iniciar y parar el software de clúster

- inicio de un clúster, Iniciar, parar, reiniciar, y borrar clústeres, Cómo iniciar y detener un clúster

- manejo de servicios de alta disponibilidad, Administrar servicios de alta disponibilidad, Administrar servicios de alta disponibilidad

- manejo de servicios de alta disponibilidad, congelar y descongelar, Cómo administrar servicios de alta disponibilidad con clusvcadm, Consideraciones para el uso de las operaciones de congelar y descongelar

- parar un clúster, Iniciar, parar, reiniciar, y borrar clústeres, Cómo iniciar y detener un clúster

- reiniciar un clúster, Iniciar, parar, reiniciar, y borrar clústeres

- reinicio de un nodo de clúster, Reinicio de un nodo de clúster

- SELinux, Adición de alta disponibilidad de Red Hat y SELinux

- uniéndose a un clúster, Hacer que un nodo abandone o se una a un clúster, Hacer que un nodo abandone o se una a un clúster

administración de clúster

- cómo configurar ACPI, Cómo configurar ACPI para usar con dispositivos de valla integrados

- cómo configurariptables, Cómo habilitar puertos IP

- consideraciones generales, Consideraciones generales de configuración

- habilitar puertos IP, Cómo habilitar puertos IP

- hardware compatible, Hardware compatible

- interruptores de red y direcciones de multidifusión, Direcciones de multidifusión

- máquinas virtuales, Configuración de las máquinas virtuales en un entorno en clúster.

- ricci consideraciones, Consideraciones para ricci

- validación de configuración, Validación de configuración

Agente de dispositivos

- IBM BladeCenter, Parámetros de dispositivos de valla

agente de valla

- fence_apc, Parámetros de dispositivos de valla

- fence_apc_snmp, Parámetros de dispositivos de valla

Agente de valla

- fence_brocade, Parámetros de dispositivos de valla

- fence_cisco_ucs, Parámetros de dispositivos de valla

- fence_drac5, Parámetros de dispositivos de valla

- fence_eaton_snmp, Parámetros de dispositivos de valla

- fence_hpblade, Parámetros de dispositivos de valla

- fence_ipdu, Parámetros de dispositivos de valla

- fence_virt, Parámetros de dispositivos de valla

- IBM iPDU, Parámetros de dispositivos de valla

Agente de valla fence_brocade, Parámetros de dispositivos de valla

Agente de valla fence_cisco_ucs, Parámetros de dispositivos de valla

Agente de valla fence_drac5, Parámetros de dispositivos de valla

Agente de valla fence_hpblade, Parámetros de dispositivos de valla

Agente de valla fence_ipdu, Parámetros de dispositivos de valla

Agente de valla fence_virt, Parámetros de dispositivos de valla

Agente de valla IBM iPDU, Parámetros de dispositivos de valla

agente de valla _apc_snmp, Parámetros de dispositivos de valla

agente de vallas

- fence_cisco_mds, Parámetros de dispositivos de valla

Agente de vallas

- fence_bladecenter, Parámetros de dispositivos de valla
- fence_egenera, Parámetros de dispositivos de valla
- fence_eps, Parámetros de dispositivos de valla
- fence_ibmblade, Parámetros de dispositivos de valla
- fence_ifmib, Parámetros de dispositivos de valla
- fence_ilo, Parámetros de dispositivos de valla
- fence_ilo_mp, Parámetros de dispositivos de valla
- fence_intelmodular, Parámetros de dispositivos de valla
- fence_ipmilan, Parámetros de dispositivos de valla
- fence_rhevm, Parámetros de dispositivos de valla
- fence_rsb, Parámetros de dispositivos de valla
- fence_scsi, Parámetros de dispositivos de valla
- fence_vmware_soap, Parámetros de dispositivos de valla
- fence_wti, Parámetros de dispositivos de valla

agente de vallas fence_apc, Parámetros de dispositivos de valla

Agente de vallas fence_bladecenter, Parámetros de dispositivos de valla

Agente de vallas fence_cisco_mds, Parámetros de dispositivos de valla

Agente de vallas fence_egenera, Parámetros de dispositivos de valla

Agente de vallas fence_eps, Parámetros de dispositivos de valla

Agente de vallas fence_ibmblade, Parámetros de dispositivos de valla

Agente de vallas fence_ifmib, Parámetros de dispositivos de valla

Agente de vallas fence_ilo, Parámetros de dispositivos de valla

Agente de vallas fence_ilo_mp, Parámetros de dispositivos de valla

Agente de vallas fence_intelmodular, Parámetros de dispositivos de valla

Agente de vallas fence_ipmilan, Parámetros de dispositivos de valla

Agente de vallas fence_rhevm, Parámetros de dispositivos de valla

Agente de vallas fence_rsb, Parámetros de dispositivos de valla

Agente de vallas fence_scsi, Parámetros de dispositivos de valla

Agente de vallas fence_vmware_soap , Parámetros de dispositivos de valla

Agente de vallas fence_wti fence, Parámetros de dispositivos de valla

Alta disponibilidad, LVM, Alta disponibilidad de LVM (HA-LVM)

C

clúster

- administración, Antes de configurar la adición de alta disponibilidad de Red Hat, Administración de adición de alta disponibilidad de Red Hat con Conga, Administración de adición de alta disponibilidad de Red Hat con ccs, Administración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos

- diagnóstico y corrección de problemas, Cómo diagnosticar y corregir problemas en un clúster, Cómo diagnosticar y corregir problemas en un clúster

- iniciar, parar, reiniciar, Iniciar y parar el software de clúster

cluster administration

- NetworkManager, Consideraciones para NetworkManager

Comentarios, Comentarios

Cómo configurar alta disponibilidad de LVM, Alta disponibilidad de LVM (HA-LVM)

conducta, recursos de alta disponibilidad, Comportamiento de recursos de alta disponibilidad

configuración

- servicio de alta disponibilidad, Consideraciones para configurar servicios de alta disponibilidad

Configuración de clúster, Configuración de adición de alta disponibilidad de Red Hat con Conga, Configuración de adición de alta disponibilidad de Red Hat con el comando ccs, Configuración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos

- actualización, Cómo actualizar una configuración

- borrado o adición de un nodo, Borrar o añadir un nodo

Configuración de servicio de alta disponibilidad

- vista general, Consideraciones para configurar servicios de alta disponibilidad

Conga

- acceso, Configuración de software de adición de Alta disponibilidad de Red Hat

Conmutación de tiempo de espera, Revisión de recursos de servicios de clúster y tiempo de espera de conmutación

Cortafuegos de iptables, Cómo configurar el cortafuegos de iptables para permitir componentes de clúster

D

Detección y solución de problemas

- diagnóstico y corrección de problemas en un clúster, Cómo diagnosticar y corregir problemas en un clúster, Cómo diagnosticar y corregir problemas en un clúster

direcciones de multidifusión

- consideraciones para usar con interruptores de red y direcciones de multidifusión, Direcciones de multidifusión

disco de cuórum

- consideraciones para usar, Consideraciones para usar disco de cuórum

Dispositivo de valla

- Eaton network power switch, Parámetros de dispositivos de valla
- HP BladeSystem, Parámetros de dispositivos de valla

Dispositivo de valla Cisco UCS, Parámetros de dispositivos de valla

Dispositivo de valla de controlador Egenera SAN , Parámetros de dispositivos de valla

Dispositivo de valla de interruptor de energía WTI, Parámetros de dispositivos de valla

Dispositivo de valla HP Bladesystem, Parámetros de dispositivos de valla

Dispositivo de valla Intel Modular , Parámetros de dispositivos de valla

Dispositivo de vallas

- Cisco MDS, Parámetros de dispositivos de valla
- Cisco UCS, Parámetros de dispositivos de valla
- Controlador Egenera SAN, Parámetros de dispositivos de valla
- Dell DRAC 5, Parámetros de dispositivos de valla
- Fence virt, Parámetros de dispositivos de valla
- HP iLO MP, Parámetros de dispositivos de valla
- HP iLO/iLO2, Parámetros de dispositivos de valla
- IBM BladeCenter SNMP, Parámetros de dispositivos de valla
- IF MIB, Parámetros de dispositivos de valla
- Intel Modular, Parámetros de dispositivos de valla
- IPMI LAN, Parámetros de dispositivos de valla
- RHEV-M REST API, Parámetros de dispositivos de valla
- vallas SCSI, Parámetros de dispositivos de valla

Dispositivo de vallas CISCO MDS , Parámetros de dispositivos de valla

Dispositivo de vallas de interruptor Brocade Fabric, Parámetros de dispositivos de valla

Dispositivo de vallas Dell DRAC 5 , Parámetros de dispositivos de valla

Dispositivo de vallas Fence virt, Parámetros de dispositivos de valla

Dispositivo de vallas HP iLO MP , Parámetros de dispositivos de valla

Dispositivo de vallas HP iLO/iLO2, Parámetros de dispositivos de valla

Dispositivo de vallas IBM BladeCenter , Parámetros de dispositivos de valla

Dispositivo de vallas IBM BladeCenter SNMP, Parámetros de dispositivos de valla

Dispositivo de vallas IF MIB, Parámetros de dispositivos de valla

Dispositivo de vallas IPMI LAN, Parámetros de dispositivos de valla

Dispositivo de vallas RHEV-M REST API , Parámetros de dispositivos de valla

Dispositivo de vallas VMware (Interfaz SOAP), Parámetros de dispositivos de valla

Dispositivos de valla

- Interruptor Brocade Fabric, Parámetros de dispositivos de valla

dispositivos de valla integrados

- configuración de ACPI, Cómo configurar ACPI para usar con dispositivos de valla integrados, Parámetros de dispositivos de valla
- Interruptor de alimentación APC en telnet/SSH, Parámetros de dispositivos de valla

Dispositivos de vallas

- ePowerSwitch, Parámetros de dispositivos de valla
- Fujitsu Siemens Remoteview Service Board (RSB), Parámetros de dispositivos de valla
- Interruptor de energía WTI, Parámetros de dispositivos de valla
- VMware (Interfaz SOAP), Parámetros de dispositivos de valla

Dispositivos de vallas ePowerSwitch , Parámetros de dispositivos de valla

Dispositivos de vallas Fujitsu Siemens Remoteview Service Board (RSB), Parámetros de dispositivos de valla

E

Etiqueta de totem

- valor de consenso, El valor de consenso para totem en un clúster de dos nodos

F

fence_eaton_snmp fence agent, Parámetros de dispositivos de valla

funcionalidades, nuevas y cambiadas, Funcionalidades nuevas y cambiadas

G

general

- consideraciones para administración de clúster, Consideraciones generales de configuración

Gestores de servicio de clúster

- configuración, Adición de un servicio de clúster al clúster, Adición de un servicio de clúster al clúster, Adición de un servicio de clúster al clúster

H

hardware

- compatible, Hardware compatible

herramientas, línea de comandos, Resumen de herramientas de línea de comandos

I

Interruptor de alimentación APC en dispositivo de valla de telnet/SSH , Parámetros de dispositivos de valla

Interruptor de alimentación APC en dispositivos de valla SNMP, Parámetros de dispositivos de valla

Interruptor de energía de red Eaton, Parámetros de dispositivos de valla

Introducción, Introducción

introducción

- otros documentos de Red Hat Enterprise Linux, Introducción

iptables

- configuración, Cómo habilitar puertos IP

M

máquinas virtuales, en un clúster, Configuración de las máquinas virtuales en un entorno en clúster.

N

NetworkManager

- inactivo para usar con clúster, Consideraciones para NetworkManager

P

parámetros, dispositivo de valla, Parámetros de dispositivos de valla

parámetros, recursos de alta disponibilidad, Parámetros de recursos de alta disponibilidad

Puertos IP

- habilitar, Cómo habilitar puertos IP

Q

qdisk

- consideraciones para usar, Consideraciones para usar disco de cuórum

R

Recursos de clúster, revisión de estatus, Revisión de recursos de servicios de clúster y tiempo de espera de conmutación

relaciones

- recursos de clúster, Relaciones padre, hijo y hermanos entre recursos

relaciones de recursos de clúster, Relaciones padre, hijo y hermanos entre recursos

Revisión de estatus de recursos de clúster, Revisión de recursos de servicios de clúster y tiempo de espera de conmutación

ricci

- consideraciones para administración de clúster, Consideraciones para ricci

S

SELinux

- configuración, Adición de alta disponibilidad de Red Hat y SELinux

servicios de clúster, Adición de un servicio de clúster al clúster, Adición de un servicio de clúster al clúster

- (ver también adición a la configuración de clúster)

Servicios de clúster, Adición de un servicio de clúster al clúster

- (ver también añadiendo a la configuración del cluster)

software de clúster

- configuración, Configuración de adición de alta disponibilidad de Red Hat con Conga, Configuración de adición de alta disponibilidad de Red Hat con herramientas de línea de comandos

Software de clúster

- configuración, Configuración de adición de alta disponibilidad de Red Hat con el comando ccs

T

tablas

- parámetros, dispositivos de vallas, Parámetros de dispositivos de valla

- recursos de alta disponibilidad, parámetros, Parámetros de recursos de alta disponibilidad

Tiempo de espera de conmutación, Revisión de recursos de servicios de clúster y tiempo de espera de conmutación

tipos

- recurso de clúster, Consideraciones para configurar servicios de alta disponibilidad

Tipos de recursos de clúster, Consideraciones para configurar servicios de alta disponibilidad

V

validación

- configuración de clúster, Validación de configuración

Vallas SCSI, Parámetros de dispositivos de valla

Valor de consenso, **El valor de consenso para totem en un clúster de dos nodos**

Visión general

- funcionalidades, nuevas y cambiadas, Funcionalidades nuevas y cambiadas