Red Hat Enterprise Linux 6

Guía de configuración de vallas

Cómo configurar y administrar dispositivos de cercado de alta disponibilidad

Last Updated: 2018-04-16

Red Hat Enterprise Linux 6 Guía de configuración de vallas

Cómo configurar y administrar dispositivos de cercado de alta disponibilidad

.

Legal Notice

Resumen

El cercado es la desconexión de un nodo del almacenamiento compartido de clúster. El cercado corta la E/S del almacenamiento compartido, lo cual asegura la integridad de los datos. Este manual documenta la configuración de cercado en sistemas en clúster mediante el complemento de alta disponibilidad y detalla la configuración de los dispositivos de vallas.

Table of Contents

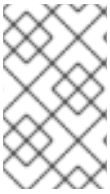
CAPÍTULO 1. PRECONFIGURACIÓN DE CERCADO

Este capítulo describe las tareas a realizar y las consideraciones a tener en cuenta antes de implementar el cercado en clústeres mediante Red Hat High Availability Add-On; consta de las siguientes secciones:

- Sección 1.1, “Cómo configurar ACPI para usar con dispositivos de vallas integrados”

1.1. CÓMO CONFIGURAR ACPI PARA USAR CON DISPOSITIVOS DE VALLAS INTEGRADOS

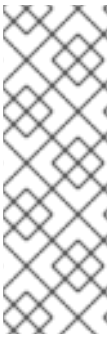
Si su clúster usa dispositivos de vallas integrados, debe configurar ACPI (Configuración avanzada e Interfaz de Energía) para asegurar cercado inmediato y completo.



NOTA

Para obtener información más actualizada sobre dispositivos de vallas integrados soportados por Red Hat High Availability Add-On, consulte http://www.redhat.com/cluster_suite/hardware/.

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

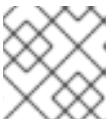


NOTA

El tiempo necesario para cercar un nodo depende del dispositivo de vallas integrado que se utilice. Algunos dispositivos de vallas integrados realizan el equivalente de presionar y sostener el botón de encendido; por lo tanto, el dispositivo de vallas apaga el nodo en cuatro o cinco segundos. Otros dispositivos de vallas integrados realizan el equivalente de presionar el botón de encendido momentáneamente, confiando en que el sistema operativo apague el nodo; por lo tanto, el dispositivo de vallas apaga el nodo en un lapso 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 para desactivar ACPI Soft-Off es con administración **`chkconfig`**, sin embargo, si ese método no es satisfactorio para su clúster, desactive ACPI Soft-Off con alguno de los siguientes métodos:

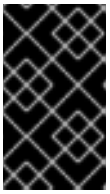
- Cambiar la configuración de BIOS a "instant-off" o una configuración equivalente que apague el nodo sin demora



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

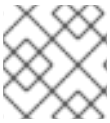
Este método inhabilita completamente a ACPI; algunos computadores no arrancan correctamente si ACPI se inhabilita totalmente. Use este método *solamente* si otros métodos no son efectivos para su clúster.

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

- La Sección 1.1.1, “Desactivar ACPI Soft-Off con administración de **chkconfig** ” — Método preferido
- La Sección 1.1.2, “Desactivar ACPI Soft-Off con el BIOS” — Primer método alterno
- La Sección 1.1.3, “Desactivar completamente a ACPI en el archivo **grub.conf**” — Segundo método alterno

1.1.1. Desactivar ACPI Soft-Off con administración de chkconfig

Utilice administración de **chkconfig** para desactivar ACPI Soft-Off, ya sea quitando el daemon ACPI (**acpid**) de la administración de **chkconfig** o apagando **acpid**.



NOTA

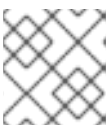
Este es el método preferido para desactivar ACPI Soft-Off.

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. Si el clúster esté configurado y ejecutándose, verifique si el nodo se apaga inmediatamente cuando está cercado.



NOTA

Cerque el nodo con el comando **fence_node** o **Conga**.

1.1.2. Desactivar ACPI Soft-Off con el BIOS

Administración de **chkconfig** (Sección 1.1.1, “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.

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

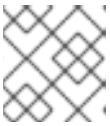
1. Reinicie el nodo e inicie el programa **`BIOS CMOS Setup Utility`**.
2. Navegue al menú de **Energía** (o el equivalente al menú de administración de energía).
3. En el menú de **Energía**, configure la función (o equivalente) **Soft-Off by PWR-BTTN** a **Apagado instantáneo** (o configuración equivalente que apague el nodo con el botón de energía sin demora). El Ejemplo 1.1, "**`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 por PWR-BTTN** establecida a **Apagado instantáneo**.

   NOTA

   Los equivalentes a la **Función ACPI**, **Soft-Off by PWR-BTTN**,y **Apagado instantáneo** varían entre computadores. Sin embargo, el objetivo de este procedimiento es configurar el BIOS para que el computador se apague sin retraso mediante el botón de energía.

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

   NOTA

   Cerque el nodo con el comando **`fence_node`** o **Conga**.

Ejemplo 1.1. `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**.

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

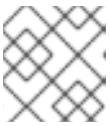
La administración de **chkconfig** (Sección 1.1.1, “Desactivar ACPI Soft-Off con administración de **chkconfig** ”), es el método preferido para desactivar ACPI Soft-Off. Si el método preferido no es efectivo para su clúster, desactive ACPI Soft-Off con la administración de energía BIOS (Sección 1.1.2, “Desactivar ACPI Soft-Off con el BIOS”). Si ninguno de los dos métodos es efectivo para su clúster, desactive 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.

Para desactivar ACPI completamente, edite 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 1.2, “Línea de comandos de arranque de Kernel con **acpi=off** añadida”).
3. Reinicie el nodo.
4. Si el clúster esté configurado y ejecutándose, verifique si el nodo se apaga inmediatamente cuando está cercado.



NOTA

Cerque el nodo con el comando **fence_node** o **Conga**.

Ejemplo 1.2. 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".

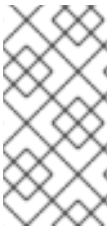
CAPÍTULO 2. CONFIGURACIÓN DE CERCADO CON EL COMANDO CCS

A partir del lanzamiento de Red Hat Enterprise Linux 6.1, Red Hat High Availability Add-On 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**. Use el comando **ccs** para configurar un archivo de configuración de clúster en un sistema de archivos local o un nodo remoto. El 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 clúster Red Hat High Availability Add-On mediante el comando **ccs**.

Este capítulo consta de las siguientes secciones:

- Sección 2.1, “Cómo configurar dispositivos de vallas”



NOTA

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.

NOTA

Este capítulo hace referencia a los elementos y atributos más utilizados de **cluster.conf**. 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**).

2.1. CÓMO CONFIGURAR DISPOSITIVOS DE VALLAS

La configuración de dispositivos de vallas consiste en crear, actualizar y borrar dispositivos de vallas para el clúster. Debe crear y nombrar los dispositivos de vallas en un clúster antes de configurar el cercado para los nodos en el clúster. Par obtener más información sobre configuración de cercado para los nodos individuales en el clúster, consulte la Sección 2.3, “Cómo configurar cercado para miembros de clúster”.

Antes de configurar sus dispositivos de vallas, debería modificar algunas de las propiedades de daemon de vallas para su sistema de los valores predeterminados. Los valores que configure para el daemon 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 daemon de vallas (**fenced**) espera antes de cercar un nodo (un miembro de un dominio de vallas) 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 daemon de vallas (**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 daemon.

Por ejemplo, para configurar el valor para el atributo **post_fail_delay**, ejecute el siguiente comando. Este comando sobrescribe los valores de las demás propiedades del daemon de vallas existentes que usted haya establecido con este comando.

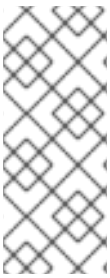
```
ccs -h host --setfencedaemon post_fail_delay=valor
```

Por ejemplo, para configurar el valor del atributo **post_join_delay**, ejecute el siguiente comando. Este comando sobrescribe los valores de las demás propiedades del daemon de vallas existentes que usted haya establecido con este comando.

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

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 más información sobre los atributos **post_join_delay** y **post_fail_delay** y de las propiedades del daemon de vallas adicionales que usted puede modificar, consulte la página de manual fenced(8) y vaya al esquema de clúster 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 vallas para un clúster, ejecute el siguiente comando:

```
ccs -h host --addfencedev
nombre_de_dispositivo
[opciones_de_dispositivos_de_cercado]
```

Por ejemplo, para configurar un dispositivo de vallas 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 vallas APC:

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

–

Cuando configure los dispositivos de vallas para un clúster, es útil ver el listado de los dispositivos disponibles para su clúster y las opciones para cada dispositivo. También le puede ser útil ver el listado de dispositivos de vallas actualmente configurados para su clúster. Si desea obtener información sobre el uso del comando **ccs** para imprimir la lista de dispositivos de vallas disponibles y opciones o para imprimir la lista de los dispositivos de vallas configurados actualmente, consulte la Sección 2.2, “Cómo listar dispositivos de vallas y opciones de dispositivos de vallas ”.

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

```
ccs -h host --rmfencedev nombre_de_dispositivo_de_vallas
```

Por ejemplo, para retirar un dispositivo de vallas 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 vallas que usted ya ha configurado, debe primero retirar ese dispositivo de vallas y luego añadirlo de nuevo con los atributos modificados.

Observe que cuando haya terminado de configurar todos los componentes de su clúster, deberá sincronizar el archivo de configuración de clúster para todos los nodos.

2.2. CÓMO LISTAR DISPOSITIVOS DE VALLAS Y OPCIONES DE DISPOSITIVOS DE VALLAS

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

Para imprimir la 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 vallas, ejecute el siguiente comando:

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

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 vallas actualmente configurados para su clúster, ejecute el siguiente comando:

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

2.3. CÓMO CONFIGURAR CERCADO PARA MIEMBROS DE CLÚSTER

Una vez haya completado los pasos iniciales de creación de un clúster y dispositivos de vallas, necesitará configurar el cercado para los nodos de clúster. Para configurar el cercado para los nodos después de crear un nuevo clúster y de configurar los dispositivos de vallas 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 2.3.1, “Cómo configurar un dispositivo de vallas basado en energía simple para un nodo”
- Sección 2.3.2, “Cómo configurar un dispositivo de vallas basado en almacenamiento simple para un nodo”
- Sección 2.3.3, “Cómo configurar un dispositivo de vallas de respaldo”
- Sección 2.3.4, “Cómo configurar un nodo con energía redundante”
- Sección 2.3.6, “Cómo retirar métodos de vallas e instancias de vallas ”

2.3.1. Cómo configurar un dispositivo de vallas basado en energía simple para un nodo

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

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

   ```
   ccs -h host --addmethod método nodo
   ```

   Por ejemplo, para configurar un método de vallas 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 vallas 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 nombre_de_dispositivo_de_vallas nodo
   method [opciones]
   ```

   Por ejemplo, para configurar una instancia de vallas 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 vallas llamado **apc** para nodo de cluster de vallas **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
   ```

-

Necesitará un método de vallas para cada nodo en el cluster. Los siguientes comandos configuran un método de vallas para cada nodo con el nombre del método **APC**. El dispositivo para el método de vallas 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 2.1, "Cómo configurar dispositivos de vallas". 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 2.1, "**cluster.conf** después de añadir métodos de vallas 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 2.1. cluster.conf después de añadir métodos de vallas 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 haya terminado de configurar todos los componentes de su clúster, deberá sincronizar el archivo de configuración de clúster para todos los nodos.

2.3.2. Cómo configurar un dispositivo de vallas basado en almacenamiento simple para un nodo

Al utilizar métodos de vallas sin-energía (es decir SAN/cercado de almacenamiento) para nodo de vallas, debe configurar *unfencing* para el dispositivo de vallas. 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 vallas correspondiente que ha configurado para el nodo con la adición notable de una acción explícita de **on** o **enable**.

Para obtener más 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 vallas de almacenamiento simple que utiliza un dispositivo de vallas denominado **sanswitch1**, el cual usa el agente de cercado **fence_sanbox2**.

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

   ```
   ccs -h host --addmethod método nodo
   ```

   Por ejemplo, para configurar un método de vallas 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 vallas 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 nombre_de_dispositivo_de_vallas nodo
   method [opciones]
   ```

   Por ejemplo, para configurar una instancia de vallas 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 vallas llamado **sanswitch1** para nodo de cluster de vallas **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 nombre_de_dispositivo_de_vallas nodo
   action=on|off
   ```

Debe añadir un método de vallas para cada nodo en el clúster. Los siguientes comandos configuran un método para cada nodo con el nombre del método **SAN**. El dispositivo para método de vallas especifica

sanswitch como el nombre de dispositivo, el cual es un dispositivo configurado anteriormente con la opción --addfencedev, como se describió en la Sección 2.1, “Cómo configurar dispositivos de vallas”. 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 2.2, “**cluster.conf** Después de adicionar métodos de vallas 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 2.2. cluster.conf Después de adicionar métodos de vallas basados en almacenamientos

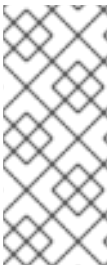
```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="SAN">
       <device name="sanswitch1" port="11"/>
            </method>
         </fence>
         <unfence>
             <device name="sanswitch1" 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 haya terminado de configurar todos los componentes de su clúster, deberá sincronizar el archivo de configuración de clúster para todos los nodos.

2.3.3. Cómo configurar un dispositivo de vallas 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 vallas 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 la lista de los métodos de vallas e instancias configuradas actualmente para un nodo si ejecuta el siguiente comando. Si no especifica el nodo, este comando listará los métodos de vallas e instancias actualmente configurados para todos los nodos.

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

Siga el siguiente procedimiento para configurar un nodo con un método de vallas primario que utiliza un dispositivo de vallas llamado **apc**, el cual usa el agente de vallas **fence_apc** y un dispositivo de cercado de respaldo con un dispositivo de vallas 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 vallas para ese dispositivo.

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

   ```
   ccs -h host --addmethod método nodo
   ```

Por ejemplo, para configurar un método de vallas 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. Agregue una instancia de vallas para método primario. Debe especificar el dispositivo de vallas 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 nombre_de_dispositivo_de_vallas nodo
method [opciones]
```

Por ejemplo, para configurar una instancia de vallas 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 vallas llamado **apc** para nodo de cluster de vallas **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 método de vallas de respaldo para el nodo, proporcionando un nombre para el método de vallas.

```
ccs -h host --addmethod método nodo
```

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

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

4. Añada una instancia de vallas para el método de respaldo. Debe especificar el dispositivo de vallas 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 nombre_de_dispositivo_de_vallas nodo
method [opciones]
```

Por ejemplo, para configurar una instancia de vallas 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 vallas llamado **sanswitch1** para nodo de cluster de vallas **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
```

Continúe añadiendo métodos de vallas cuando sea necesario.

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

Ejemplo 2.3, "**cluster.conf** Después de añadir métodos de vallas 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 clúster.

Ejemplo 2.3. cluster.conf Después de añadir métodos de vallas 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 haya terminado de configurar todos los componentes de su clúster, deberá sincronizar el archivo de configuración de clúster para todos los nodos.

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 clúster. El primer método que usted 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, retire el método de cercado primario del archivo de configuración y agréguelo de nuevo.

2.3.4. 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 vallas 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 vallas 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 vallas 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 vallas para el cluster. Para obtener más información sobre cómo configurar dispositivos de vallas, consulte la Sección 2.1, “Cómo configurar dispositivos de vallas”.

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

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

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

   ```
   ccs -h host --addmethod método nodo
   ```

Por ejemplo, para configurar un método de vallas 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 vallas para la primera fuente de alimentación a un método de vallas. Debe especificar el dispositivo de vallas 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 nombre_de_dispositivo_de_vallas nodo
method [opciones] action=off
```

Por ejemplo, para configurar una instancia de vallas 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 vallas para la segunda fuente de alimentación al método de vallas. Debe especificar el dispositivo de vallas 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 nombre_de_dispositivo_de_vallas nodo
method [opciones] action=off
```

Por ejemplo, para configurar una segunda instancia de vallas 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 vallas denominado **apc2** para nodo de cluster de vallas **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 vallas, configurando el atributo **action** como **on**. Debe especificar el dispositivo de vallas 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 vallas 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 vallas 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 vallas especificando el atributo **action** como **on** para esta instancia. Debe especificar el dispositivo de vallas 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 vallas 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 vallas denominado **apc2** para nodo de clúster de vallas **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 2.4, "**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 2.4. 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 haya terminado de configurar todos los componentes de su clúster, deberá sincronizar el archivo de configuración de clúster para todos los nodos.

2.3.5. Prueba de configuración de cercado

A partir del lanzamiento de Red Hat Enterprise Linux 6.4, usted puede probar la configuración de vallas para cada nodo en un clúster con la herramienta **fence_check**.

El siguiente comando muestra la salida de una ejecución correcta de este comando:

```
[root@host-098 ~]# fence_check
fence_check run at Wed Jul 23 09:13:57 CDT 2014 pid: 4769
Testing host-098 method 1: success
Testing host-099 method 1: success
Testing host-100 method 1: success
```

Para obtener información sobre esta herramienta, consulte la página de manual **fence_check**(8).

2.3.6. Cómo retirar métodos de vallas e instancias de vallas

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

```
ccs -h host --rmmethod method nodo
```

Por ejemplo, para retirar un método de vallas 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 vallas de un dispositivo de un método de vallas, ejecute el siguiente comando:

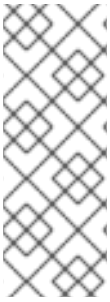
```
ccs -h host --rmfenceinst nombre_de_dispositivo_de_vallas nodo método
```

Por ejemplo, para retirar todas las instancias del dispositivo de vallas 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
```

CAPÍTULO 3. CONFIGURACIÓN DE CERCADO CON CONGA

Este capítulo describe cómo configurar el cercado en Red Hat High Availability Add-On mediante **Conga**.



NOTA

Conga es una interfaz gráfica de usuario que sirve para administrar la adición de Red Hat High Availability Add-On. No obstante, observe que para usar efectivamente la interfaz usted debe 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 el sistema puede no ser lo suficientemente sólido para mantener todos los servicios en ejecución cuando los componentes fallen.

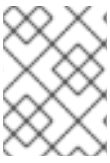
3.1. CONFIGURACIÓN DE PROPIEDADES DE DAEMON DE VALLAS

Al hacer clic en la pestaña **Daemon de vallas** aparece la página **Propiedades de daemon de vallas**, 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 vallas específicos para los nodos del clúster, use el elemento del menú **Dispositivos de vallas** de la pantalla de clúster, como se describe en la Sección 3.2, “Cómo configurar dispositivos de vallas”.

- El parámetro de **Retraso de posfalla** es el número de segundos que un daemon de vallas (**`fenced`**) espera antes de cercar un nodo (un miembro de dominio de vallas) después de que el nodo haya fallado. El **retraso de posfalla** 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 daemon de vallas (**`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 más información sobre el **Retraso de posconexión** y el **Retraso de posfalla**, consulte la página de manual fenced(8).

3.2. CÓMO CONFIGURAR DISPOSITIVOS DE VALLAS

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.

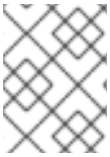
La creación de un dispositivo de vallas consiste en seleccionar un tipo de dispositivo de vallas e ingresar parámetros para ese dispositivo de vallas (por ejemplo, nombre, dirección IP, inicio de sesión y contraseña). La actualización de un dispositivo de vallas consiste en seleccionar un dispositivo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

existente y cambiar los parámetros para ese dispositivo de vallas. La eliminación de un dispositivo de vallas consiste en seleccionar un dispositivo existente de la vallas y la eliminación.

Esta sección provee procedimientos para las siguientes tareas:

- La creación de dispositivos de vallas — Consulte la Sección 3.2.1, “Cómo crear un dispositivo de vallas”. Cuando haya creado y nombrado un dispositivo de vallas, puede configurar los dispositivos de vallas para cada nodo en el clúster, así como se describe en la Sección 3.3, “Cómo configurar cercado para miembros de clúster”.
- Actualización de dispositivos de vallas — Consulte la Sección 3.2.2, “Modificación de un dispositivo de vallas”.
- Borrado de servicios de vallas — Consulte la Sección 3.2.3, “Borrado de un dispositivo de vallas”.

Desde la página específica de clúster, puede configurar los dispositivos de vallas para ese clúster, si hace clic en **Dispositivos de vallas** en la parte superior de la pantalla de clúster. Así muestra los dispositivos de vallas para el clúster y muestra los elementos de menú para configuración de dispositivos de vallas: **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 vallas, y por lo tanto, no se muestra ninguno.

Figura 3.1, “Página de configuración de dispositivos de vallas Luci ” muestra dispositivos de vallas de pantalla de configuración antes de que cualquier dispositivo de vallas haya sido creado.

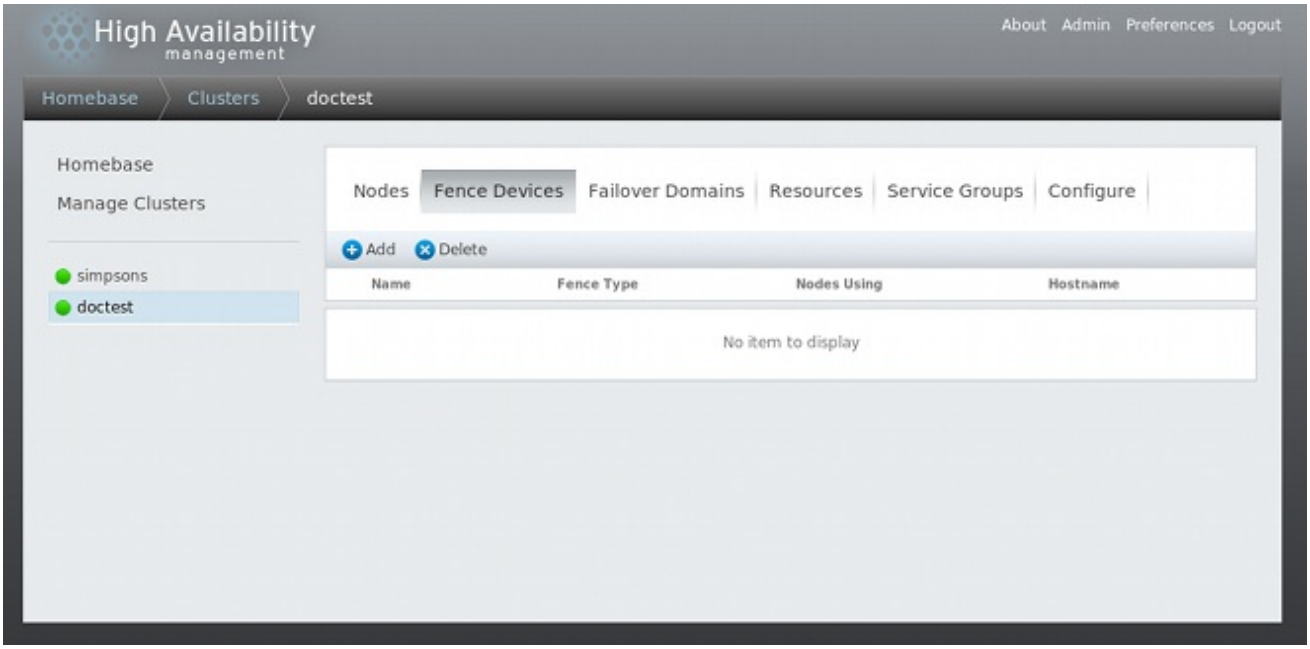


Figura 3.1. Página de configuración de dispositivos de vallas Luci

3.2.1. Cómo crear un dispositivo de vallas

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

1. Desde la página de configuración **Dispositivos de vallas**, haga clic en **Añadir**. Al hacer clic en **Añadir** aparece el cuadro de diálogo **Añadir dispositivo de vallas (instancia)**. Desde este cuadro de diálogo, seleccione el tipo de dispositivo de vallas a configurar.

2. Especifique la información en el cuadro de diálogo **Añadir un dispositivo de vallas (instancia)** según el tipo de dispositivo de valla. En algunos casos deberá especificar parámetros específicos de nodos adicionales para el dispositivo de vallas para configurar el cercado de nodos individuales.

3. Haga clic en **Enviar**.

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

3.2.2. Modificación de un dispositivo de vallas

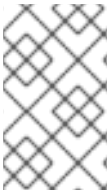
Para modificar un dispositivo de vallas, siga los siguientes pasos:

1. Desde la página de configuración **Dispositivos de vallas**, haga clic en el nombre de dispositivo de vallas a modificar. Este muestra el cuadro de diálogo para el dispositivo de vallas, con los valores que han sido configurados para el dispositivo.

2. Para modificar el dispositivo de vallas, ingrese los cambios para los parámetros desplegados.

3. Haga clic en **Aplicar** y espere a que la configuración se actualice.

3.2.3. Borrado de un dispositivo de vallas



NOTA

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

Para borrar un dispositivo de vallas, 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 vallas 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 vallas eliminado ya no aparece en la pantalla.

3.3. CÓMO CONFIGURAR CERCADO PARA MIEMBROS DE CLÚSTER

Una vez haya completado los pasos iniciales de creación de un clúster y dispositivos de vallas, configure el cercado para los nodos de clúster. Siga los pasos en esta sección, para configurar el cercado para los nodos después de crear un clúster y de configurar los dispositivos de vallas para el clúster. Observe que debe configurar el cercado para cada nodo en el clúster.

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

- Sección 3.3.1, “Configuración de un dispositivo de vallas único para un nodo”
- Sección 3.3.2, “Cómo configurar un dispositivo de vallas de respaldo”
- Sección 3.3.3, “Cómo configurar un nodo con energía redundante”

3.3.1. 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 el nodo.

   La página específica de nodo muestra los servicios que están ejecutándose en el nodo, así como también los dominios de conmutación de los cuales este nodo es un miembro. Para modificar un dominio de conmutación, haga clic en su nombre.

3. En la página específica de nodo, bajo **Dispositivos de vallas**, haga clic en **`Añadir método de vallas`**. Este desplegará el cuadro de diálogo **`Añadir método de vallas 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 Red Hat High Availability Add-On. 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 vallas para este método al hacer clic en el botón **`Añadir una instancia de vallas`**. De esta manera se muestra el menú desplegable **Añadir dispositivo de vallas (Instancia)** desde el cual puede seleccionar un dispositivo de vallas que anteriormente haya configurado, como se describe en la Sección 3.2.1, “Cómo crear un dispositivo de vallas”.

7. Seleccione un dispositivo de vallas para este método. Si este dispositivo de vallas requiere que usted configure los parámetros de nodos específicos, la pantalla muestra los parámetros que debe configurar.

NOTA

Para métodos de vallas 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 más información sobre quitar la vallas 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.

3.3.2. Cómo configurar 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 3.3.1, “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 vallas**.

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 vallas para este método al hacer clic en **Añadir una instancia de vallas**. De esta manera se muestra un menú desplegable desde el cual puede seleccionar un dispositivo de vallas que anteriormente ha configurado, como se describe en la Sección 3.2.1, “Cómo crear un dispositivo de vallas”.

5. Seleccione un dispositivo de vallas para este método. Si este dispositivo de vallas requiere que usted configure los parámetros de nodos específicos, la pantalla muestra los parámetros que debe configurar.

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

Continúe 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**.

3.3.3. Cómo configurar 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 vallas 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 vallas 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.

Para configurar el cercado para un nodo con abastecimiento de energía dual, siga los pasos a continuación en estas 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 vallas para el clúster. Para obtener más información sobre parámetros, consulte la Sección 3.2, “Cómo configurar dispositivos de vallas”.

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. 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**.

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 el nodo.

4. En la página específica de nodo, haga clic en **`Añadir un método de vallas`**.

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 vallas 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 3.2.1, “Cómo crear un dispositivo de vallas”.

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 3.2.1, “Cómo crear un dispositivo de vallas”.

11. Seleccione el segundo de los dispositivos de vallas 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 vallas e instancias de vallas desplegadas, mostrando que cada dispositivo apagará el sistema en secuencia y encenderá el sistema en secuencias. Esto se muestra en la Figura 3.2, “Configuración de cercado de doble energía”.

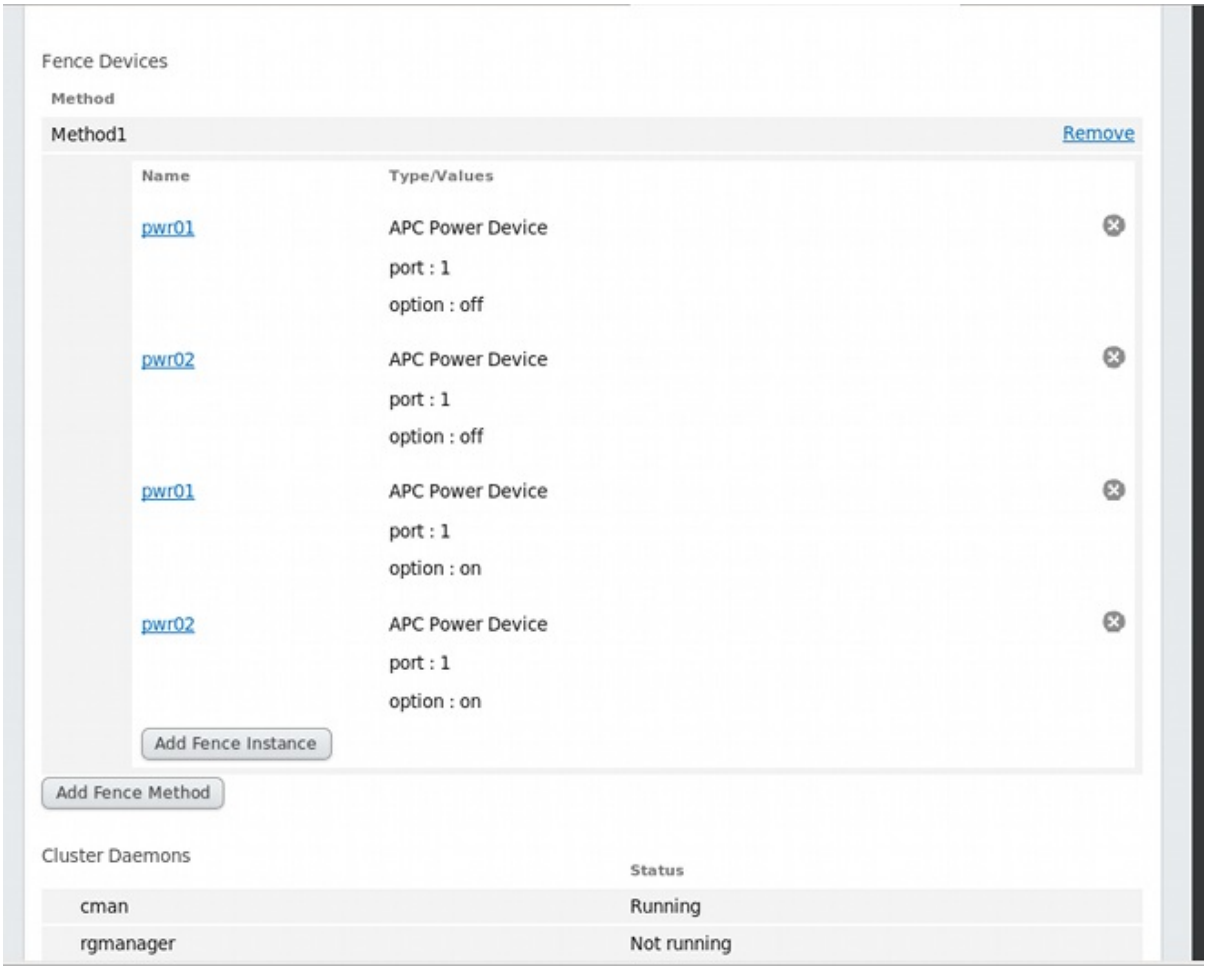


Figura 3.2. Configuración de cercado de doble energía

3.3.4. Prueba de configuración de cercado

A partir del lanzamiento de Red Hat Enterprise Linux 6.4, usted puede probar la configuración de vallas para cada nodo en un clúster con la herramienta **fence_check**.

El siguiente comando muestra la salida de una ejecución correcta de este comando:

```
[root@host-098 ~]# fence_check
fence_check run at Wed Jul 23 09:13:57 CDT 2014 pid: 4769
Testing host-098 method 1: success
Testing host-099 method 1: success
Testing host-100 method 1: success
```

Para obtener información sobre esta herramienta, consulte la página de manual **fence_check**(8).

CAPÍTULO 4. DISPOSITIVOS DE VALLAS

Este capítulo documenta los dispositivos de vallas que reciben soporte actualmente en Red Hat Enterprise Linux High-Availability Add-On.

La Tabla 4.1, “Resumen de dispositivos de vallas” lista los dispositivos de vallas, los agentes de dispositivos de vallas asociados con los dispositivos de vallas, y provee una referencia para la tabla que documenta los parámetros para los dispositivos de vallas.

Tabla 4.1. Resumen de dispositivos de vallas

Dispositivo de vallas	Agente de vallas	Referencia para descripción de parámetros
Interruptor APC (Telnet/SSH)	fence_apc	Tabla 4.2, “Interruptor APC (Telnet/SSH)”
Interruptor de alimentación APC en SNMP	fence_apc_snmp	Tabla 4.3, “Interruptor de alimentación APC en SNMP”
Interruptor Brocade Fabric	fence_brocade	Tabla 4.4, “Interruptor Brocade Fabric”
Cisco MDS	fence_cisco_mds	Tabla 4.5, “Cisco MDS”
Cisco UCS	fence_cisco_ucs	Tabla 4.6, “Cisco UCS”
Dell DRAC 5	fence_drac5	Tabla 4.7, “Dell DRAC 5”
Dell iDRAC	fence_idrac	Tabla 4.22, “LAN IPMI (Interfaz de administración de plataforma inteligente), Dell iDrac, IBM Integrated Management Module, HPiLO3, HPiLO4.”
Interruptor de energía de red Eaton (Interfaz SNMP).	fence_eaton_snmp	Tabla 4.8, “El controlador de energía de red Eaton (Controlador SNMP) (Red Hat Enterprise Linux 6.4 y posteriores)”
Egenera BladeFrame	fence_egenera	Tabla 4.9, “Egenera BladeFrame”
ePowerSwitch	fence_eps	Tabla 4.10, “ePowerSwitch”
Fence kdump	fence_kdump	Tabla 4.11, “Valla kdump”
Fence virt	fence_virt	Tabla 4.12, “Fence virt”

Dispositivo de vallas	Agente de vallas	Referencia para descripción de parámetros
Fujitsu Siemens Remoteview Service Board (RSB)	fence_rsb	Tabla 4.13, “Fujitsu Siemens Remoteview Service Board (RSB)”
HP BladeSystem	fence_hpblade	Tabla 4.14, “HP BladeSystem (Red Hat Enterprise Linux 6.4 y posterior)”
HP iLO Device (Integrated Lights Out),	fence_ilo	Tabla 4.15, “HP iLO (Integrated Lights Out) y HP iLO2”
HP iLO2	fence_ilo2	Tabla 4.15, “HP iLO (Integrated Lights Out) y HP iLO2”
HPiLO3	fence_ilo3	Tabla 4.22, “LAN IPMI (Interfaz de administración de plataforma inteligente), Dell iDrac, IBM Integrated Management Module, HPiLO3, HPiLO4.”
HPiLO4	fence_ilo4	Tabla 4.22, “LAN IPMI (Interfaz de administración de plataforma inteligente), Dell iDrac, IBM Integrated Management Module, HPiLO3, HPiLO4.”
HP iLO (Integrated Lights Out) MP	fence_ilo_mp	Tabla 4.16, “HP iLO (Integrated Lights Out) MP”
IBM BladeCenter	fence_bladecenter	Tabla 4.17, “IBM BladeCenter”
IBM BladeCenter SNMP	fence_ibmblade	Tabla 4.18, “IBM BladeCenter SNMP”
IBM Integrated Management Module	fence_imm	Tabla 4.22, “LAN IPMI (Interfaz de administración de plataforma inteligente), Dell iDrac, IBM Integrated Management Module, HPiLO3, HPiLO4.”
IBM iPDU	fence_ipdu	Tabla 4.19, “IBM iPDU (Red Hat Enterprise Linux 6.4 y posterior)”

Dispositivo de vallas	Agente de vallas	Referencia para descripción de parámetros
IF MIB	fence_ifmib	Tabla 4.20, “IF MIB”
Intel Modular	fence_intelmodular	Tabla 4.21, “Intel Modular”
LAN IPMI (Interfaz de administración de plataforma inteligente)	fence_ipmilan	Tabla 4.22, “LAN IPMI (Interfaz de administración de plataforma inteligente), Dell iDrac, IBM Integrated Management Module, HPiLO3, HPiLO4.”
RHEV-M REST API	fence_rhevm	Tabla 4.23, “RHEV-M REST API (RHEL 6.2 y versiones posteriores RHEV 3.0 y versiones posteriores)”
Cercado SCSI	fence_scsi	Tabla 4.24, “Cercado de reservaciones SCSI ”
vallas de VMware (Interfaz SOAP)	fence_vmware_soap	Tabla 4.25, “vallas de VMware (Interfaz SOAP) (Red Hat Enterprise Linux 6.2 y posterior)”
WTI Power Switch	fence_wti	Tabla 4.26, “WTI Power Switch”

4.1. INTERRUPTOR DE ENERGÍA APC SOBRE TELNET Y SSH)

Tabla 4.2, “Interruptor APC (Telnet/SSH)” lista los parámetros de vallas de dispositivos por **`fence_apc`**, el agente de vallas para APC en Telnet/SSH.

Tabla 4.2. 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 daemon de vallas 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 puerto predeterminado es 23 o 22 si selecciona **`Use SSH`**

Campo luci	Atributo `cluster.conf`	Descripción
Inicio de sesión	**`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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Espera de energía (segundos)	**`power_wait`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número de intentos de encendido. El valor predeterminado es 1.
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.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.
Usar SSH	**`secure`**	Indica que el sistema utilizará SSH para acceder al dispositivo. Cuando use SSH, debe especificar ya sea la contraseña, el script de la contraseña o un archivo de identidad.
Opciones de SSH	**`ssh_options`**	Opciones SSH a usar. El valor predeterminado es **`-1 -c blowfish`**.

Campo luci	Atributo `cluster.conf`	Descripción
Ruta al archivo de identidad SSH	**`identity_file`**	El archivo de identidad para SSH.

Figura 4.1, “WTI Power Switch” muestra la pantalla de configuración para adicionar un Agente de aislamiento para interruptores de energía APC.

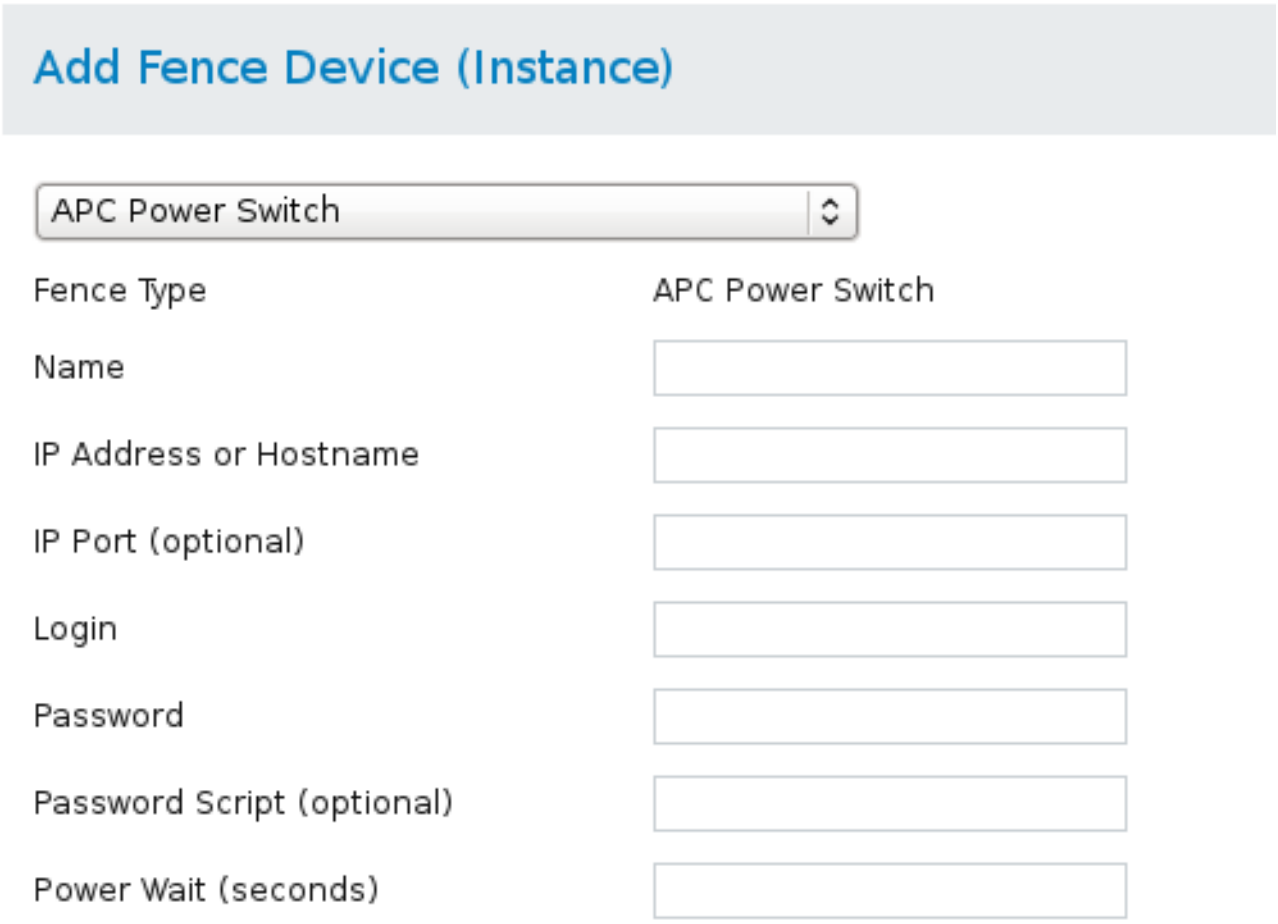


Figura 4.1. WTI Power Switch

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo APC.

```
ccs -f cluster.conf --addfencedev apc agent=fence_apc ipaddr=192.168.0.1
login=root passwd=password123
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_apc`**.

```
 <fencedevices>
   <fencedevice agent="fence_apc" name="apc" ipaddr="apc-
telnet.example.com" login="root" passwd="password123"/>
 </fencedevices>
```

4.2. INTERRUPTOR DE ALIMENTACIÓN APC EN SNMP

La Tabla 4.3, “Interruptor de alimentación APC en SNMP” lista los parámetros de dispositivo de vallas utilizados por **fence_apc_snmp**, el agente de vallas para APC que se registra en el dispositivo SNP a través del protocolo SNP.

Tabla 4.3. 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 daemon de vallas 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.
Inicio de sesión	**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 vallas. 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).

Campo luci	Atributo `cluster.conf`	Descripción
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`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número de intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	El puerto.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

Figura 4.2, “Interruptor de alimentación APC en SNMP” muestra la pantalla de configuración para adicionar un Agente de aislamiento para interruptores de energía APC.

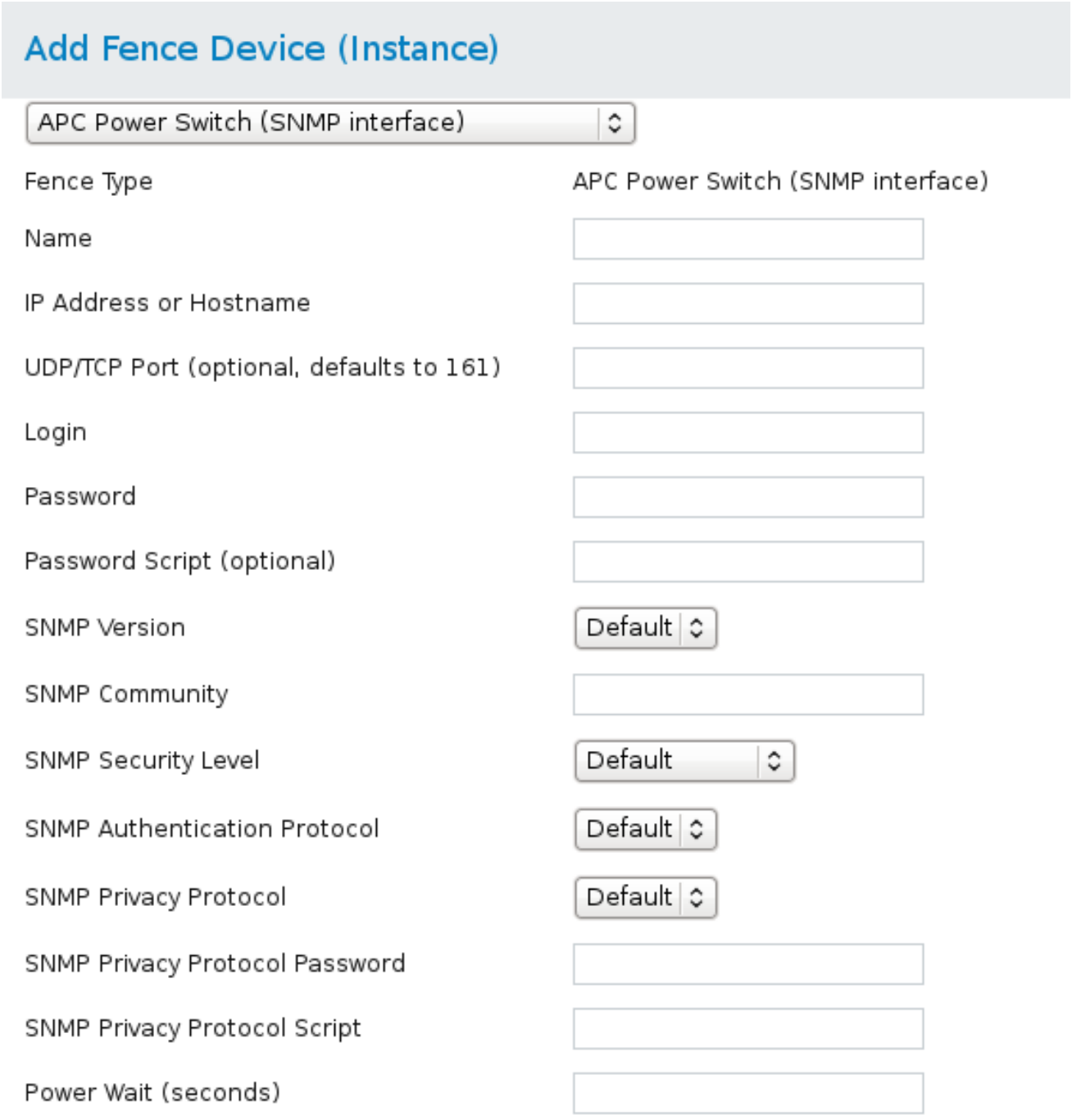


Figura 4.2. Interruptor de alimentación APC en SNMP

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_apc_snmp`** :

```
 <fencedevice>
  <fencedevice agent="fence_apc_snmp" community="private"
ipaddr="192.168.0.1" login="root" \n    name="apcpwsnmptst1"
passwd="password123" power_wait="60" snmp_priv_passwd="password123"/>
 </fencedevices>
```

4.3. INTERRUPTOR BROCADE FABRIC

La Tabla 4.4, “Interruptor Brocade Fabric” lista los parámetros de dispositivos de vallas utilizados por **`fence_brocade`**, el agente de vallas para interruptores Brocade FC.

Tabla 4.4. 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.
Inicio de sesión	**`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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Force IP Family	**`inet4_only`**, **`inet6_only`**	Fuerza al agente a usar direcciones IPv4 o IPv6 únicamente
Forzar el indicador de comandos	**`cmd_prompt`**	The command prompt to use. The default value is '\$'.
Power wait (segundos)	**`power_wait`**	Número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número de intentos de encendido. El valor predeterminado es 1.
Puerto	**`port`**	El número de salida de interruptor.

Campo luci	Atributo `cluster.conf`	Descripción
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.
Usar SSH	**`secure`**	Indica que el sistema utilizará SSH para acceder al dispositivo. Cuando use SSH, debe especificar ya sea la contraseña, el script de la contraseña o un archivo de identidad.
Opciones de SSH	**`ssh_options`**	Opciones SSH a usar. El valor predeterminado es **`-1 -c blowfish`**.
Ruta al archivo de identidad SSH	**`identity_file`**	El archivo de identidad para SSH.
Unfencing	Sección **`unfence`** del archivo de configuración de clúster.	Cuando está activado, asegura que el nodo cercado no se reactive sino hasta que haya sido reiniciado. Esto se requiere para los métodos de valla sin energía: cercado de almacenamiento y SAN. Si debe configurar un dispositivo sin cercado, primero detenga el clúster y toda la configuración, incluidos los dispositivos y agregue sin cercado antes de iniciar el clúster. Para obtener más información, consulte la página de manual **`fence_node`**(8).

La Figura 4.3, “Interruptor Brocade Fabric” muestra la pantalla de configuración para adicionar un dispositivo de vallas Brocade Fabric Switch.

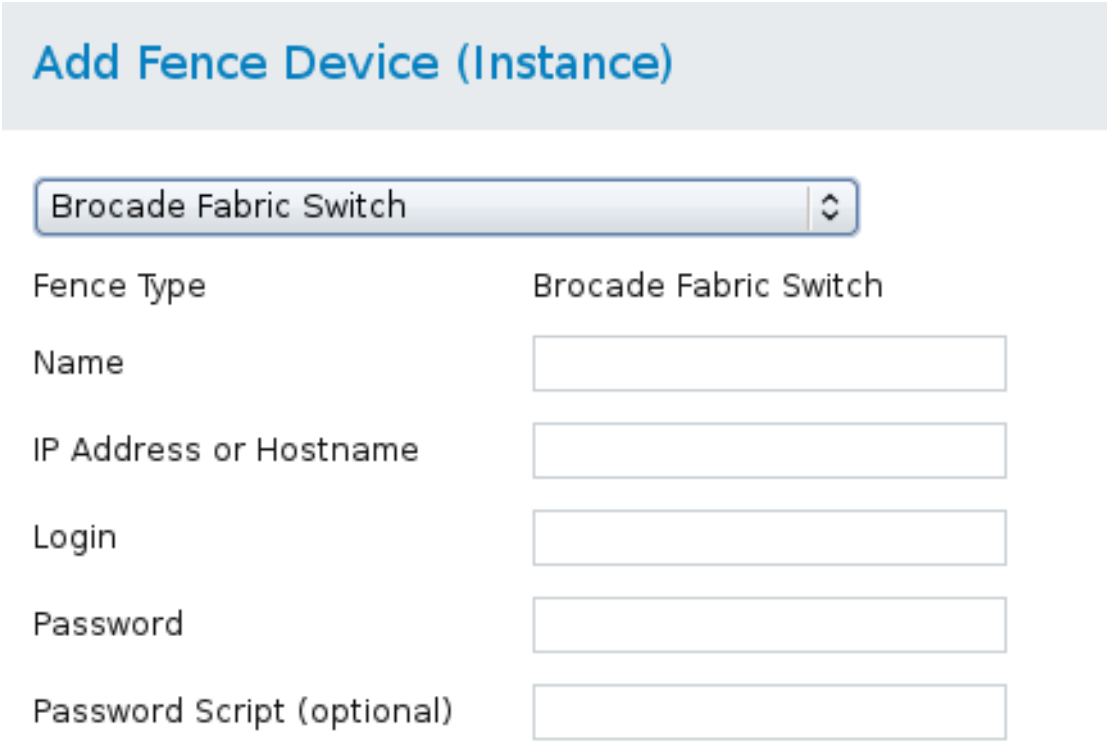


Figura 4.3. Interruptor Brocade Fabric

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo Brocade.

```
ccs -f cluster.conf --addfencedev brocadetest agent=fence_brocade
ipaddr=brocadetest.example.com login=root \n passwd=password123
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_brocade`** :

```
 <fencedevices>
  <fencedevice agent="fence_brocade" ipaddr="brocadetest.example.com"
login="brocadetest" \n    name="brocadetest" passwd="brocadetest"/>
 </fencedevices>
```

4.4. CISCO MDS

La Tabla 4.5, “Cisco MDS” lista los parámetros de vallas utilizados por **`fence_cisco_mds`**, el agente de vallas para Cisco MDS.

Tabla 4.5. Cisco MDS

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	**`name`**	Un nombre para el dispositivo series 9000 Cisco MDS con SNMP habilitado.

Campo luci	Atributo `cluster.conf`	Descripción
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.
Inicio de sesión	**`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 vallas. Su uso remplaza el parámetro de **Contraseña**.
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**.
Power wait (segundos)	**`power_wait`**	El número de segundos de espera después de expedir un comando de apagado o encendido.

Campo luci	Atributo `cluster.conf`	Descripción
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de veces para la operación de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	El puerto.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.4, “Cisco MDS” muestra la pantalla de configuración para adicionar un dispositivo de vallas Cisco MDS.

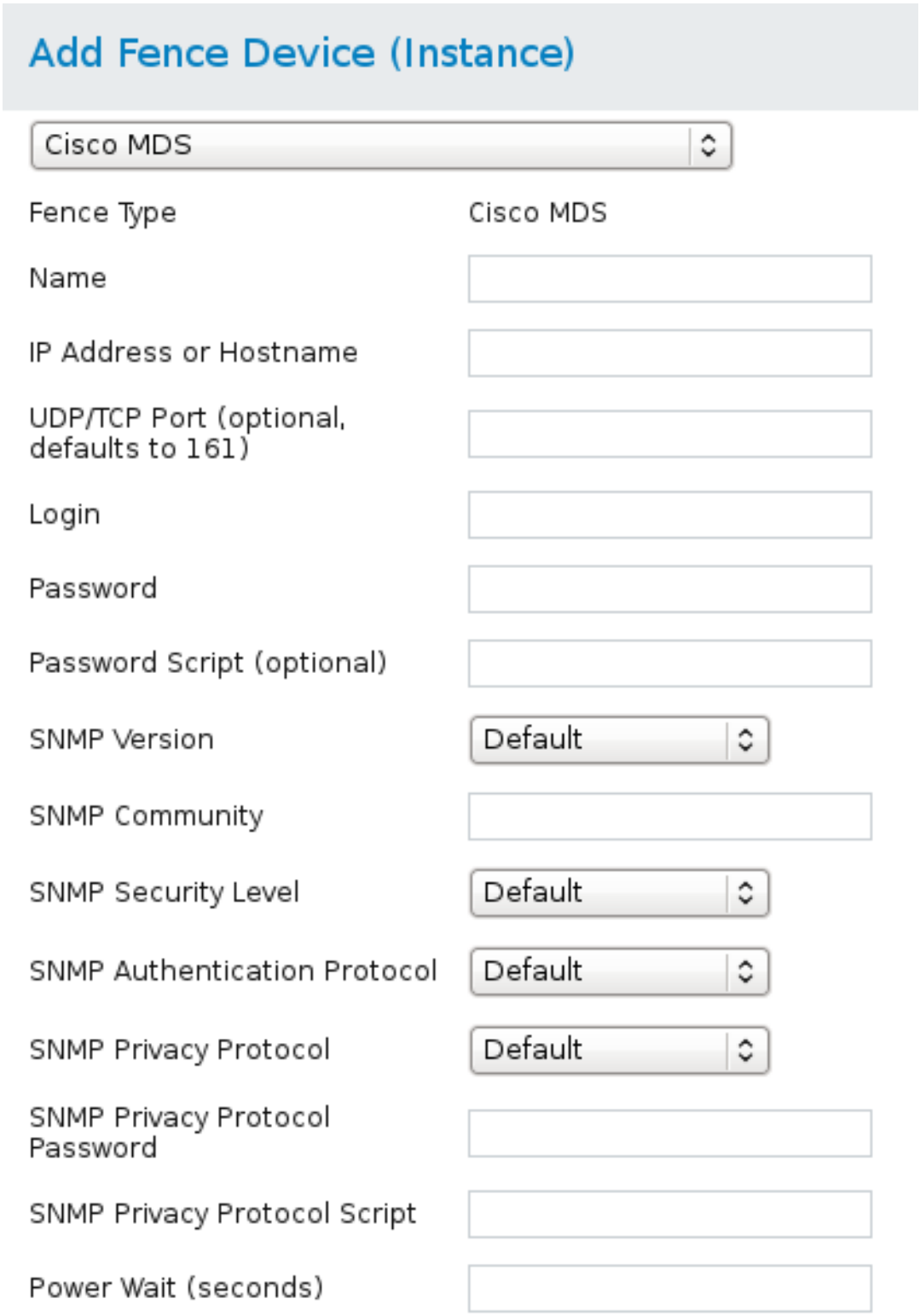


Figura 4.4. Cisco MDS

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo Cisco MDS.

```
ccs -f cluster.conf --addfencedev mds agent=fence_cisco_mds
ipaddr=192.168.0.1 name=ciscomdstest1 login=root \n passwd=password123
power_wait=60 snmp_priv_passwd=password123 udpport=161
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_cisco_mds`** :

```
 <fencedevices>
   <fencedevice agent="fence_cisco_mds" community="private"
ipaddr="192.168.0.1" login="root" \n     name="ciscomdstest1"
passwd="password123" power_wait="60" snmp_priv_passwd="password123" \n
udpport="161"/>
 </fencedevices>
```

4.5. CISCO UCS

La Tabla 4.6, “Cisco UCS” lista los parámetros de dispositivo de vallas utilizados por **`fence_cisco_ucs`**, el agente de vallas para Cisco UCS.

Tabla 4.6. 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.
Inicio de sesión	**`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 vallas. 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.
Power wait (segundos)	**`power_wait`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.

Campo luci	Atributo `cluster.conf`	Descripción
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	Nombre de la máquina virtual
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.5, “Cisco UCS” muestra la pantalla de configuración para adicionar un dispositivo de vallas Cisco UCS.

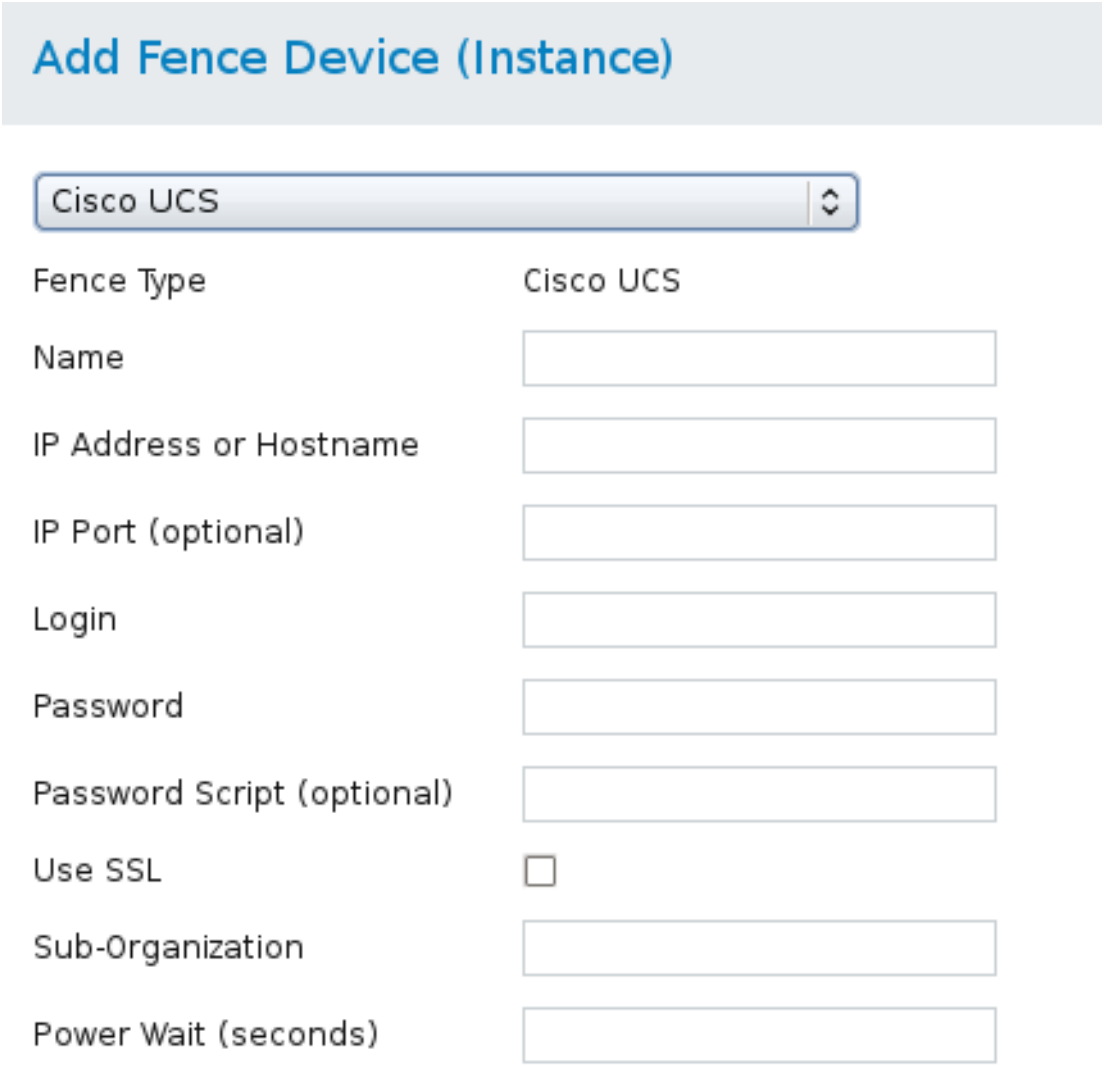


Figura 4.5. Cisco UCS

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo Cisco UCS.

```
ccs -f cluster.conf --addfencedev ucs agent=fence_cisco_ucs
ipaddr=192.168.0.1 login=root passwd=password123 \n suborg=/org-RHEL/org-
Fence/
```

El siguiente es un ejemplo de entrada **`cluster.conf`** para el dispositivo **`fence_cisco_ucs`** creado mediante Conga o con el comando **`ccs`**:

```
 <fencedevices>
  <fencedevice agent="fence_cisco_ucs" ipaddr="192.168.0.1" login="root"
name="ciscoucstest1" \n    passwd="password123" power_wait="60" ssl="on"
suborg="/org-RHEL/org-Fence/"/>
 </fencedevices>
```

4.6. DELL DRAC 5

La Tabla 4.7, “Dell DRAC 5” lista los parámetros de dispositivos de vallas utilizados por **fence_drac5**, el agente de vallas para Dell DRAC 5.

Tabla 4.7. 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.
Inicio de sesión	**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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Usa SSH	**secure**	Indica que el sistema utilizará SSH para acceder al dispositivo. Cuando use SSH, debe especificar ya sea la contraseña, el script de la contraseña o un archivo de identidad.
Opciones de SSH	**ssh_options**	Opciones SSH a usar. El valor predeterminado es **-1 -c blowfish**.
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**	The command prompt to use. The default value is '\$'.
Power wait (segundos)	**power_wait**	Número de segundos de espera después de expedir un comando de apagado o encendido.
Retraso (segundos)	**delay**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

Campo luci	Atributo `cluster.conf`	Descripción
Tiempo límite de energía (segundos)	**`power_timeout`**	Número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	Número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	Número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos para la operación de encendido	**`retry_on`**	El número de intentos para la operación de encendido. El predeterminado es 1.

La Figura 4.6, “Dell Drac 5” muestra la pantalla de configuración para adicionar un dispositivo Dell Drac 5.

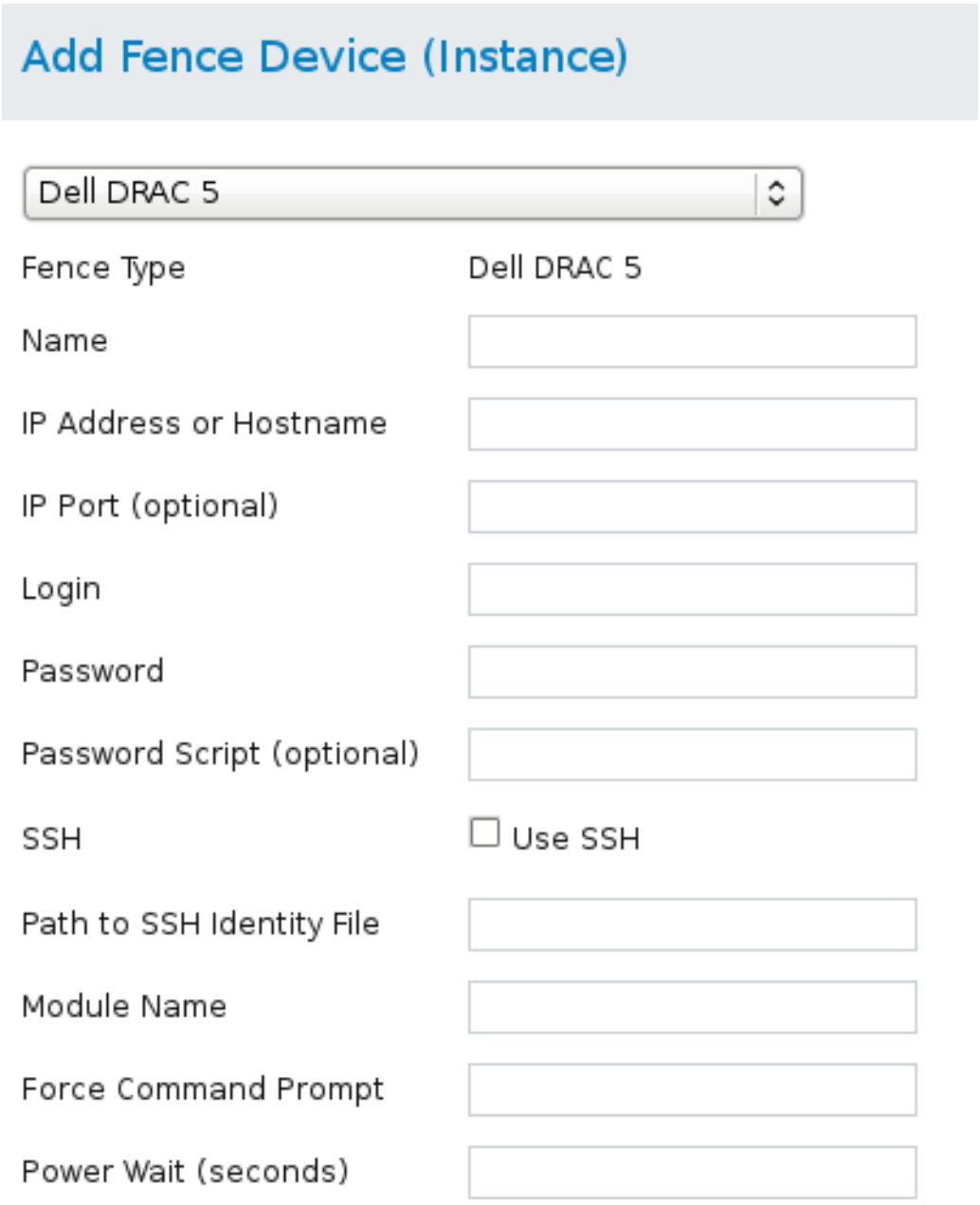


Figura 4.6. Dell Drac 5

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo Dell Drac 5.

```
ccs -f cluster.conf --addfencedev delldrac5test1 agent=fence_drac5
ipaddr=192.168.0.1 login=root passwd=password123\n module_name=drac1
power_wait=60
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_drac5`** :

```
 <fencedevices>
   <fencedevice agent="fence_drac5" cmd_prompt="\$" ipaddr="192.168.0.1"
login="root" module_name="drac1" \
     name="delldrac5test1" passwd="password123" power_wait="60"/>
 </fencedevices>
```

4.7. INTERRUPTOR DE ENERGÍA DE RED EATON

La Tabla 4.8, “El controlador de energía de red Eaton (Controlador SNMP) (Red Hat Enterprise Linux 6.4 y posteriores)” lista los parámetros del dispositivo de vallas utilizados por **`fence_eaton_snmp`**, el agente de vallas para Eaton en el interruptor de energía de red SNMP.

Tabla 4.8. 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 energía 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.
Inicio de sesión	**`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 vallas. 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).

Campo luci	Atributo `cluster.conf`	Descripción
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`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número de intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	El número de conexión física o nombre de la máquina virtual. El parámetro es obligatorio.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.7, “Interruptor de energía de red Eaton” muestra la pantalla de configuración para adicionar un dispositivo de vallas de Interruptor de energía de red Eaton.

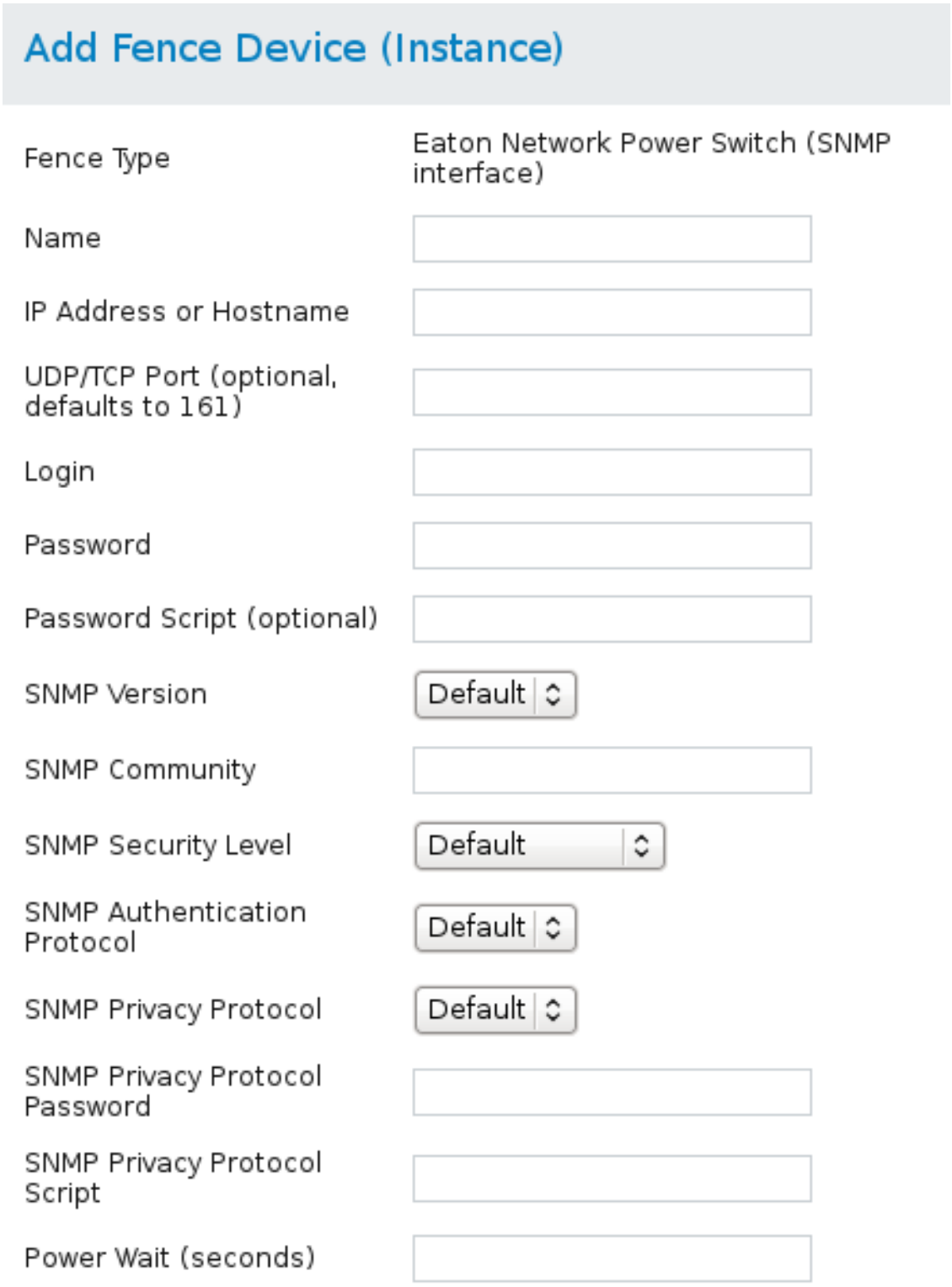


Figura 4.7. Interruptor de energía de red Eaton

El comando a continuación crea una instancia de dispositivo de vallas para un dispositivo de Interruptor de energía de red Eaton:

```
ccs -f cluster.conf --addfencedev eatontest agent=fence_eaton_snmp
ipaddr=192.168.0.1 login=root \n passwd=password123 power_wait=60
snmp_priv_passwd=eatonpassword123 udpport=161
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_eaton_snmp`** :

```
 <fencedevices>
  <fencedevice agent="fence_eaton_snmp" community="private"
ipaddr="eatonhost" login="eatonlogin" \n   name="eatontest"
passwd="password123" passwd_script="eatonpwscr" power_wait="3333" \n
snmp_priv_passwd="eatonprivprotpass"
snmp_priv_passwd_script="eatonprivprotpwscr" udpport="161"/>
 </fencedevices>
```

4.8. EGENERA BLADEFRAME

La Tabla 4.9, “Egenera BladeFrame” lista los parámetros de dispositivos de vallas utilizados por **fence_egenera**, el agente de vallas para Egenera BladeFrame.

Tabla 4.9. Egenera BladeFrame

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 más información.
Ruta ESH (opcional)	**esh**	La ruta al comando esh en el cserver (el predeterminado es /opt/pan-mgr/bin/esh)
Nombre de usuario	**user**	El nombre de ingreso. El valor predeterminado es **root**.
lpan	**lpan**	La red del área del proceso lógico (LPAN) del dispositivo.
pserver	**pserver**	El nombre de la cuchilla de procesamiento (pserver) del dispositivo.
Retraso (opcional)	**delay**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.
Sin cercado	La sección **unfence** del archivo de configuración de clúster.	Cuando está activada, asegura que el nodo cercado no se reactive sino hasta que haya sido reiniciado. Esto se requiere para los métodos de valla sin energía: cercado de almacenamiento y SAN. Si debe configurar un dispositivo sin cercado, primero detenga el clúster y toda la configuración, incluidos los dispositivos y agregue sin cercado antes de iniciar el clúster. Para obtener más información, consulte la página de manual **fence_node**(8).

La Figura 4.8, “Egenera BladeFrame” muestra la pantalla de configuración para adicionar un dispositivo de vallas Egenera BladeFrame.

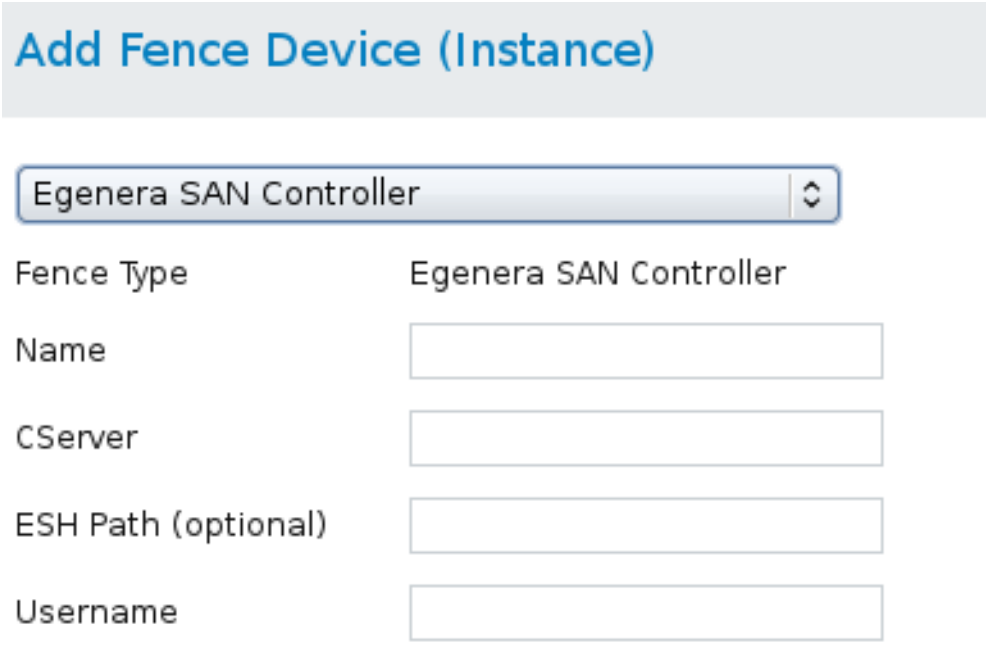


Figura 4.8. Egenera BladeFrame

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo Egenera BladeFrame :

```
ccs -f cluster.conf --addfencedev egeneratest agent=fence_egenera
user=root cserver=cservertest
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_egenera`** :

```
 <fencedevices>
  <fencedevice agent="fence_egenera" cserver="cservertest"
name="egeneratest" user="root"/>
 </fencedevices>
```

4.9. EPOWERSWITCH

La tabla Tabla 4.10, “ePowerSwitch” lista los parámetros de dispositivos de vallas utilizados por **`fence_eps`**, el agente de dispositivos para ePowerSwitch.

Tabla 4.10. 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.

Campo luci	Atributo `cluster.conf`	Descripción
Inicio de sesión	**`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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Nombre de página oculta	**`hidden_page`**	El nombre de la página oculta para el dispositivo.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	El número de conexión física o nombre de la máquina virtual.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.9, “ePowerSwitch” muestra la pantalla de configuración para adicionar un dispositivo de vallas ePowerSwitch.

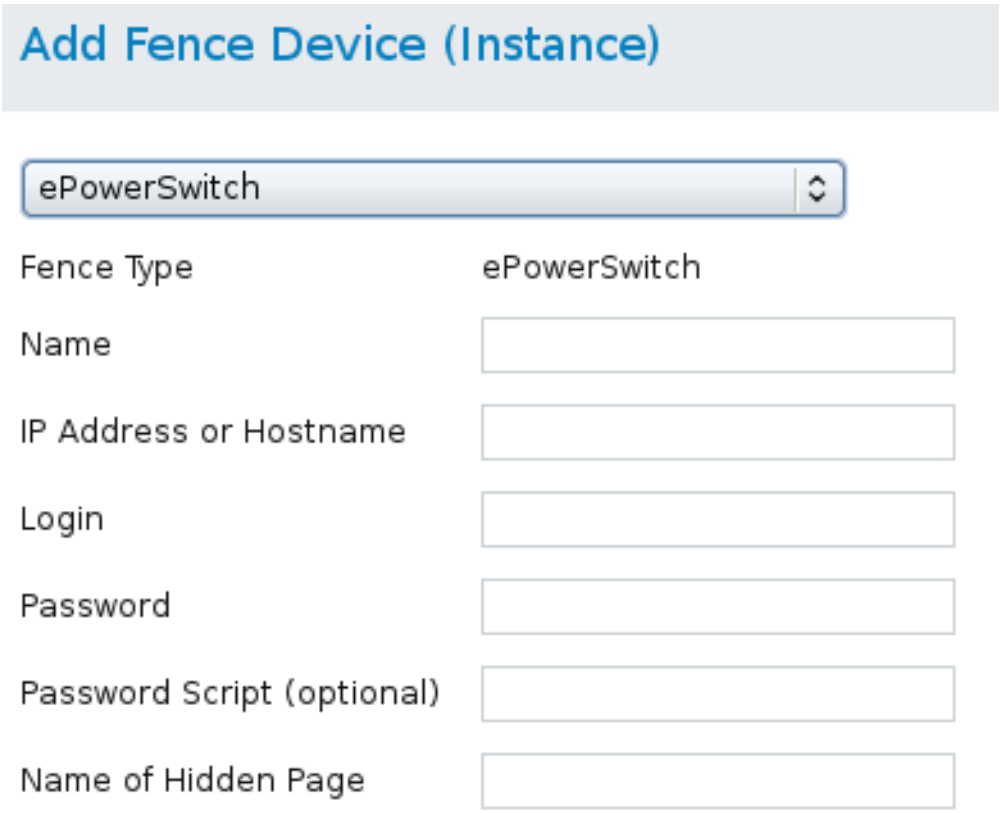


Figura 4.9. ePowerSwitch

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo ePowerSwitch.

```
ccs -f cluster.conf --addfencedev epstest1 agent=fence_eps
ipaddr=192.168.0.1 login=root passwd=password123 \n hidden_page=hidden.htm
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_eps`** :

```
 <fencedevices>
   <fencedevice agent="fence_eps" hidden_page="hidden.htm"
ipaddr="192.168.0.1" login="root" name="epstest1" \n
passwd="password123"/>
 </fencedevices>
```

4.10. VALLA KDUMP

La Tabla 4.11, “Valla kdump” lista los parámetros de dispositivo de vallas utilizados por **`fence_dkump`**, el agente de vallas para el servicio de recuperación de fallos **`kdump`**. Observe que **`fence_kdump`** no remplaza los métodos de cercado tradicionales. El agente de vallas **`fence_kdump`** únicamente detecta que un nodo ha ingresado al servicio de recuperación de fallos **`kdump`**. Esto permite que el servicio de recuperación de fallos **`kdump`** se complete sin ser interrumpido por métodos de cercado tradicionales.

Tabla 4.11. Valla kdump

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	**`name`**	Un nombre para el dispositivo **`fence_kdump`**.
Familia IP	**`family`**	Familia de red IP. El valor predeterminado es **`auto`**.
Puerto IP (opcional)	**`ipport`**	El número de puerto IP que el agente **`fence_kdump`** utilizará para escuchar mensajes. El valor predeterminado es 7410.
Operación de tiempo límite (segundos) (opcional)	**`timeout`**	Especifica el número de segundos de espera por el mensaje de nodo fallido.
Nombre de nodo	**`nodename`**	El nombre o dirección IP del nodo que va a ser cercado.

4.11. FENCE VIRT

La Tabla 4.12, “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 4.12. Fence virt

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	**`name`**	Un nombre para el dispositivo de vallas Fence virt.
Dispositivo serial	**`serial_device`**	En el host, el dispositivo serial debe ser asignado en cada archivo de configuración de dominio. Para obtener más información, consulte la página de manual **`fence_virt.conf`**. Si este campo se especifica, es el agente de vallas **`fence_virt`** que debe operar en modo serial. Al no especificar el valor el agente de vallas **`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 vallas.

Campo luci	Atributo cluster.conf	Descripción
	ipport	El puerto de canal. El valor predeterminado es 1229, el cual se utiliza para configurar el dispositivos de vallas con **luci**.
Tiempo de espera	**timeout**	Tiempo límite, en segundos. El valor predeterminado es 30.

La Figura 4.10, “Fence Virt” muestra la pantalla de configuración para adicionar un dispositivo Fence Virt.

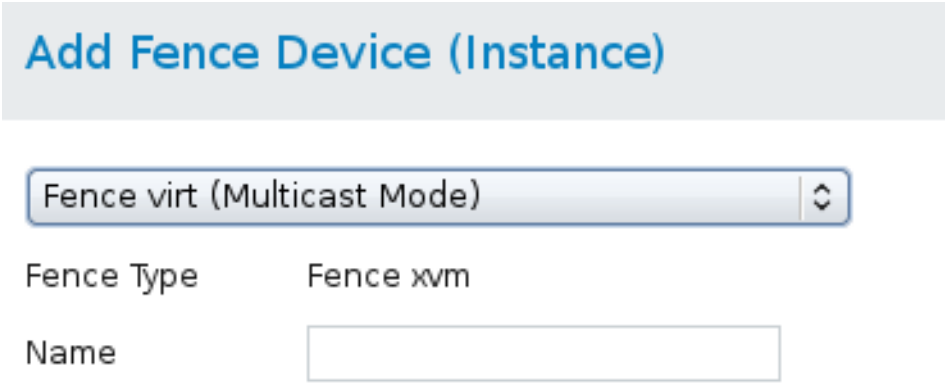


Figura 4.10. Fence Virt

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo Fence Virt :

```
ccs -f cluster.conf --addfencedev fencevirt1 agent=fence_virt
serial_device=/dev/ttyS1 serial_params=19200, 8N1
```

La siguiente es la entrada **cluster.conf** para el dispositivo **fence_virt** :

```
 <fencedevices>
   <fencedevice agent="fence_virt" name="fencevirt1"
serial_device="/dev/ttyS1" serial_params="19200, 8N1"/>
 </fencedevices>
```

4.12. FUJITSU-SIEMENS REMOTEVIEW SERVICE BOARD (RSB)

La Tabla 4.13, “Fujitsu Siemens Remoteview Service Board (RSB)” lista los parámetros de dispositivos de vallas utilizados por **fence_rsb**, el agente de vallas para Fujitsu-Siemens RemoteView Service Board (RSB).

Tabla 4.13. Fujitsu Siemens Remoteview Service Board (RSB)

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	**`name`**	Un nombre para el RSB a usar como dispositivo de vallas.
Dirección IP o nombre de host	**`ipaddr`**	El nombre de host asignado al dispositivo.
Inicio de sesión	**`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 vallas. 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.
Forzar el indicador de comandos	**`cmd_prompt`**	The command prompt to use. The default value is '\$'.
Power wait (segundos)	**`power_wait`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Retraso (segundos)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número intentos para la operación de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.

La Figura 4.11, “Fujitsu-Siemens RSB” muestra la pantalla de configuración para adicionar un dispositivo de vallas Fujitsu-Siemens RSB.

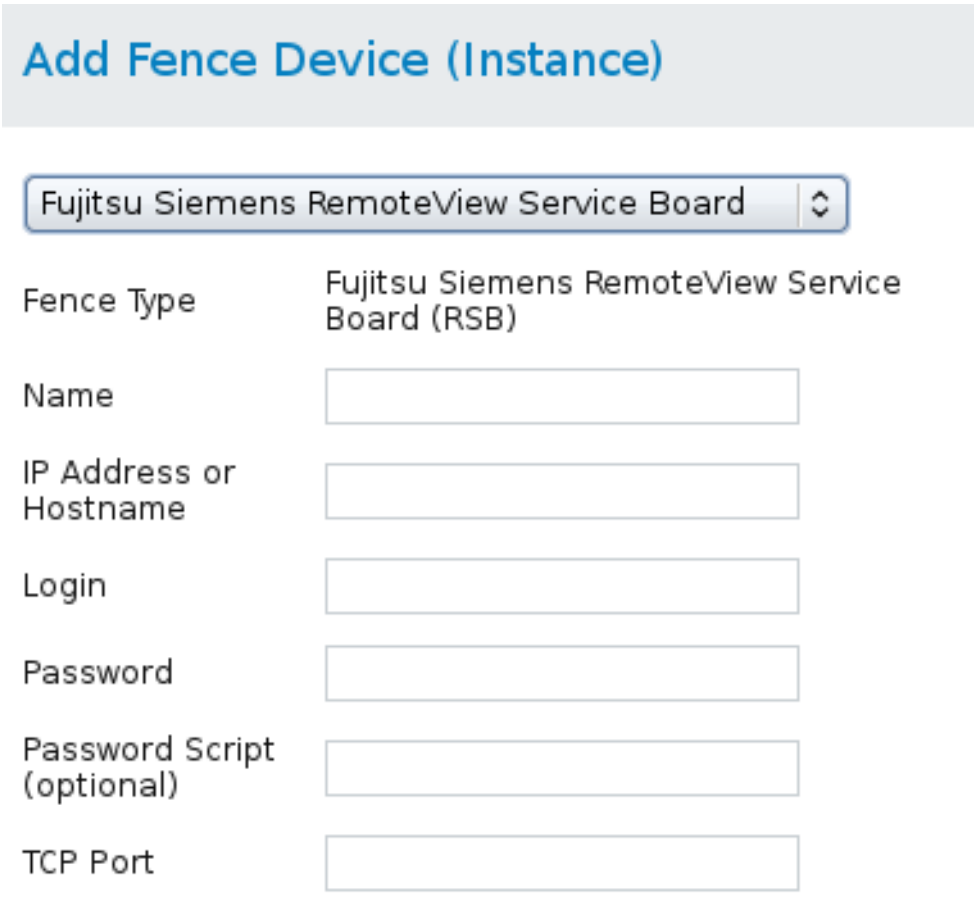


Figura 4.11. Fujitsu-Siemens RSB

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo Fujiitsu-Siemens RSB:

```
ccs -f cluster.conf --addfencedev fsrbtest1 agent=fence_rsb
ipaddr=192.168.0.1 login=root passwd=password123 \n telnet_port=3172
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_rsb`** :

```
 <fencedevices>
   <fencedevice agent="fence_rsb" ipaddr="192.168.0.1" login="root"
name="fsrsbtest1" passwd="password123" telnet_port="3172"/>
 </fencedevices>
```

4.13. HEWLETT-PACKARD BLADESYSTEM

La Tabla 4.14, “HP BladeSystem (Red Hat Enterprise Linux 6.4 y posterior)” lista los parámetros de dispositivos de vallas utilizados por **`fence_hpblade`**, el agente de vallas para HP BladeSystem.

Tabla 4.14. 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.
Inicio de sesión	**`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 vallas.
Script de contraseña (opcional)	**`passwd_script`**	El script que proporciona una contraseña para acceder al dispositivo de vallas. Su uso remplaza el parámetro de **Contraseña**.
Forzar el indicador de comandos	**`cmd_prompt`**	The command prompt to use. The default value is '\$'.
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`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Shell Timeout de shell (seconds)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo de espera de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.

Campo luci	Atributo `cluster.conf`	Descripción
El número de intentos de encendido.	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
Usa SSH	**`secure`**	Indica que el sistema utilizará SSH para acceder al dispositivo. Cuando use SSH, debe especificar ya sea la contraseña, el script de la contraseña o un archivo de identidad.
Opciones de SSH	**`ssh_options`**	Opciones SSH a usar. El valor predeterminado es **`-1 -c blowfish`**.
Ruta al archivo de identidad SSH	**`identity_file`**	El archivo de identidad para SSH.

La Figura 4.12, “HP BladeSystem” muestra la pantalla de configuración para adicionar un dispositivo de vallas HP BladeSystem.

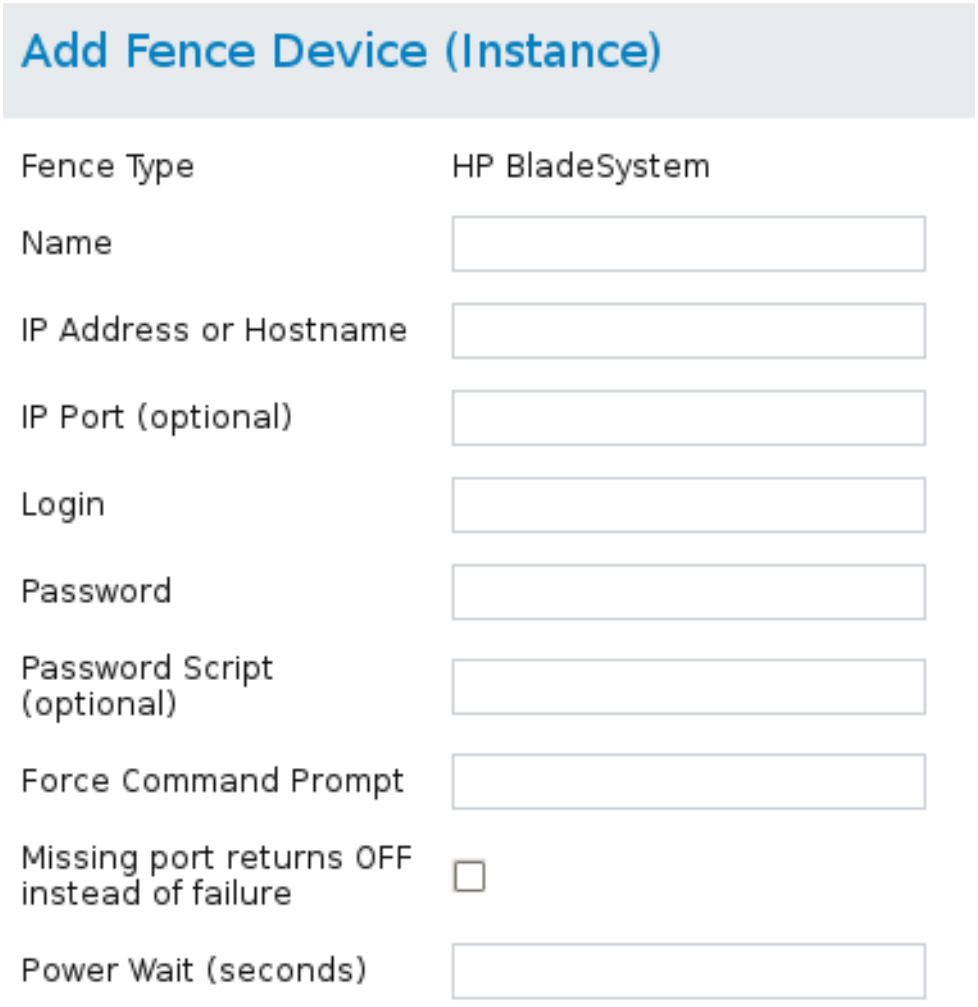


Figura 4.12. HP BladeSystem

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo BladeSystem:

```
ccs -f cluster.conf --addfencedev hpbladetest1 agent=fence_hpblade
cmd_prompt=c7000oa> ipaddr=192.168.0.1 \n login=root passwd=password123
missing_as_off=on power_wait=60
```

La siguiente es la entrada **cluster.conf** para el dispositivo **fence_hpblade** :

```
 <fencedevices>
  <fencedevice agent="fence_hpblade" cmd_prompt="c7000oa>"
ipaddr="hpbladeaddr" ipport="13456" \n   login="root" missing_as_off="on"
name="hpbladetest1" passwd="password123" passwd_script="hpbladepwscr" \n
power_wait="60"/>
 </fencedevices>
```

4.14. HEWLETT-PACKARD ILO

Los agentes de dispositivos de vallas para dispositivos HP iLO **fence_ilo** y dispositivos HP iLO2 **fence_ilo2**. comparten la misma implementación. La Tabla 4.15, “HP iLO (Integrated Lights Out) y HP iLO2” lista los parámetros de dispositivos utilizados por estos agentes.

Tabla 4.15. HP iLO (Integrated Lights Out) y HP iLO2

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**	El puerto TCP a usar para la conexión con el dispositivo, el valor predeterminado es 443.
Inicio de sesión	**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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Power wait (segundos)	**power_wait**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Retraso (segundos)	**delay**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

Campo luci	Atributo `cluster.conf`	Descripción
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.

La Figura 4.13, “HP iLO” muestra la pantalla de configuración para adicionar un dispositivo de vallas HP iLO.

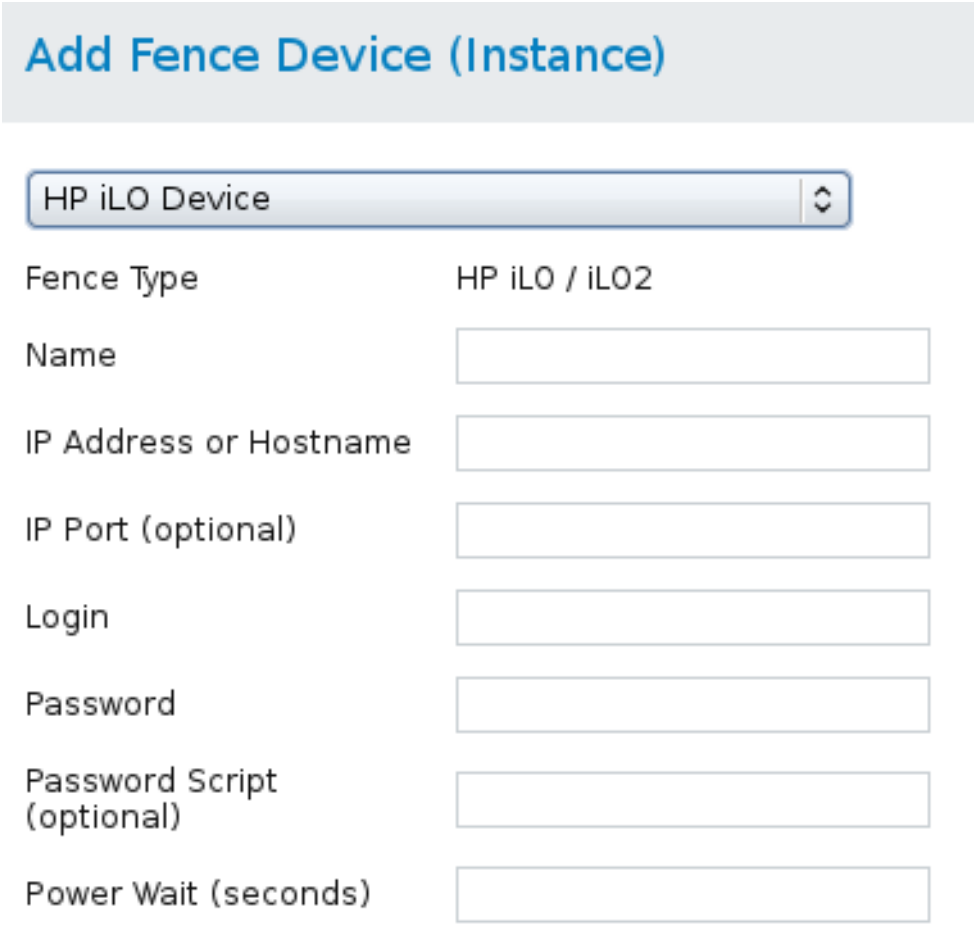


Figura 4.13. HP iLO

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo HP iLO:

```
ccs -f cluster.conf --addfencedev hpilotest1 agent=fence_hpilo
ipaddr=192.168.0.1 login=root passwd=password123 \n power_wait=60
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_ilo`** :

```
 <fencedevices>
  <fencedevice agent="fence_ilo" ipaddr="192.168.0.1" login="root"
name="hpilotest1" passwd="password123" \n   power_wait="60"/>
 </fencedevices>
```

4.15. HEWLETT-PACKARD ILO MP

La Tabla 4.16, “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 4.16. 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.
Inicio de sesión	**`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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Usa SSH	**`secure`**	Indica que el sistema utilizará SSH para acceder al dispositivo. Cuando use SSH, debe especificar ya sea la contraseña, el script de la contraseña o un archivo de identidad.
Opciones de SSH	**`ssh_options`**	Opciones SSH a usar. El valor predeterminado es **`-1 -c blowfish`**.

Campo luci	Atributo cluster.conf	Descripción
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->'.
Power wait (segundos)	power_wait	El número de segundos de espera después de emitir un comando de apagado o encendido.
Retraso (segundos)	delay	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.
Tiempo límite de energía (segundos)	power_timeout	El número de segundos de espera antes de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	shell_timeout	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	login_timeout	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de veces para la operación de encendido	retry_on	El número intentos de encendido. El valor predeterminado es 1.

La Figura 4.14, “HP iLO MP” muestra la pantalla de configuración para adicionar un dispositivo de vallas HP iLO MP.

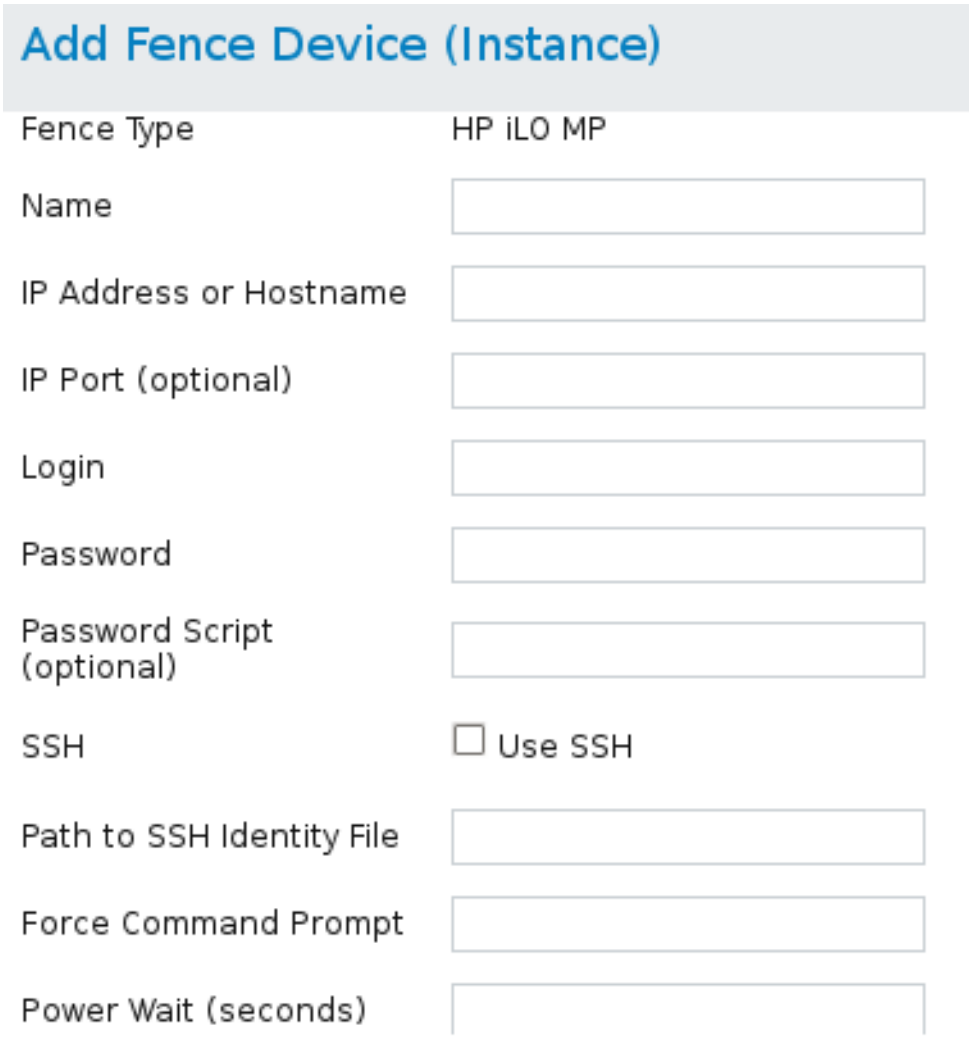


Figura 4.14. HP iLO MP

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo HP iLO MP :

```
ccs -f cluster.conf --addfencedev hpilomptest1 agent=fence_hpilo
cmd_prompt=hpiLO-> ipaddr=192.168.0.1 \n login=root passwd=password123
power_wait=60
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_hpilo_mp`** :

```
 <fencedevices>
<fencedevice agent="fence_ilo_mp" cmd_prompt="hpiLO-&gt;"
ipaddr="192.168.0.1" login="root" name="hpilomptest1" passwd="password123"
power_wait="60"/>
 </fencedevices>
```

4.16. IBM BLADECENTER

La Tabla 4.17, “IBM BladeCenter” lista los parámetros de dispositivo de vallas utilizados por **`fence_bladecenter`**, el agente de vallas para IBM BladeCenter.

Tabla 4.17. 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.
Inicio de sesión	**`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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Power wait (segundos)	**`power_wait`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
Usa SSH	**`secure`**	Indica que el sistema utilizará SSH para acceder al dispositivo. Cuando use SSH, debe especificar ya sea la contraseña, el script de la contraseña o un archivo de identidad.
Opciones de SSH	**`ssh_options`**	Opciones SSH a usar. El valor predeterminado es **`-1 -c blowfish`**.

Campo luci	Atributo `cluster.conf`	Descripción
Ruta al archivo de identidad SSH	**`identity_file`**	El archivo de identidad para SSH.

La Figura 4.15, “IBM BladeCenter” muestra la pantalla de configuración para adicionar un dispositivo de vallas IBM BladeCenter.

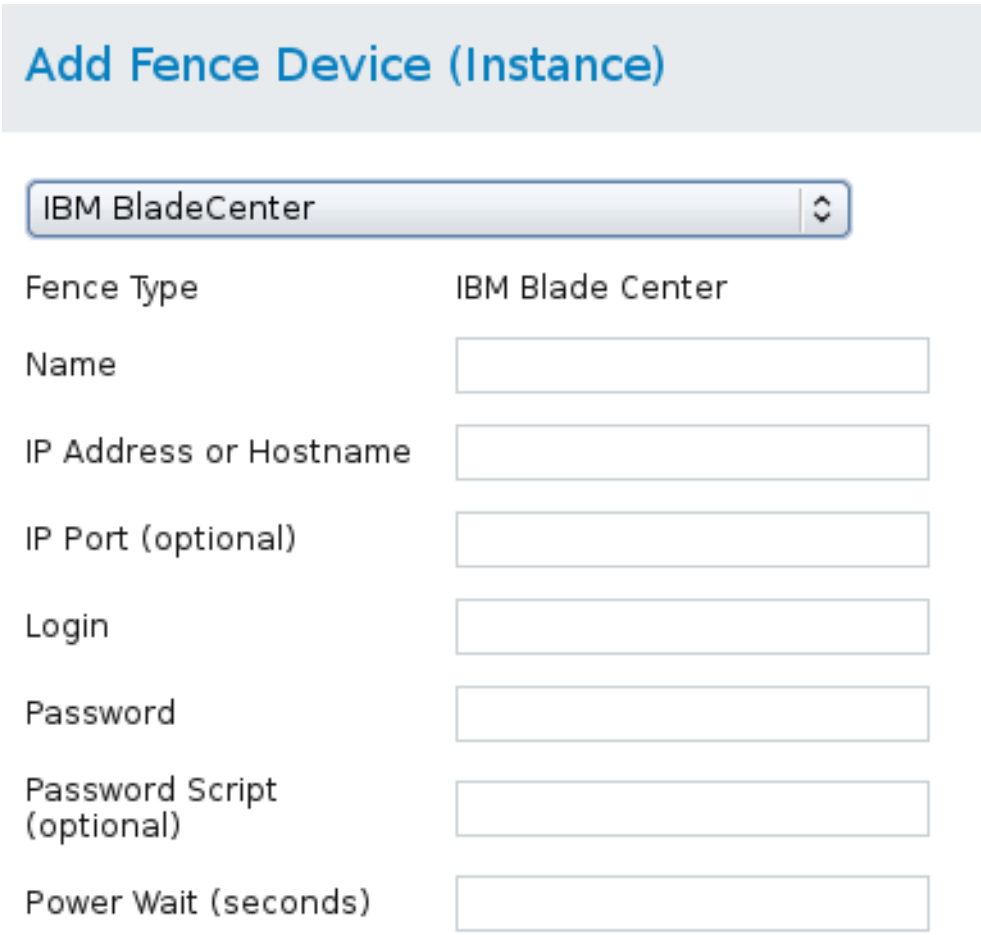


Figura 4.15. IBM BladeCenter

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo BladeCenter:

```
ccs -f cluster.conf --addfencedev bladecentertest1 agent=fence_bladecenter
ipaddr=192.168.0.1 login=root \n passwd=password123 power_wait=60
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_bladecenter`** :

```
 <fencedevices>
  <fencedevice agent="fence_bladecenter" ipaddr="192.168.0.1" login="root"
name="bladecentertest1" passwd="password123" \n   power_wait="60"/>
 </fencedevices>
```

4.17. IBM BLADECENTER SOBRE SNMP

La Tabla 4.18, “IBM BladeCenter SNMP” lista los parámetros de dispositivo de vallas utilizados por **`fence_ibmblade`**, el agente de vallas para IBM BladeCenter en SNMP.

Tabla 4.18. 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.
Inicio de sesión	**`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 vallas. 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).

Campo luci	Atributo `cluster.conf`	Descripción
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`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	El número de conexión física o nombre de la máquina virtual.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.16, “IBM BladeCenter SNMP” muestra la pantalla de configuración para adicionar un dispositivo de vallas IBM BladeCenter SNMP.

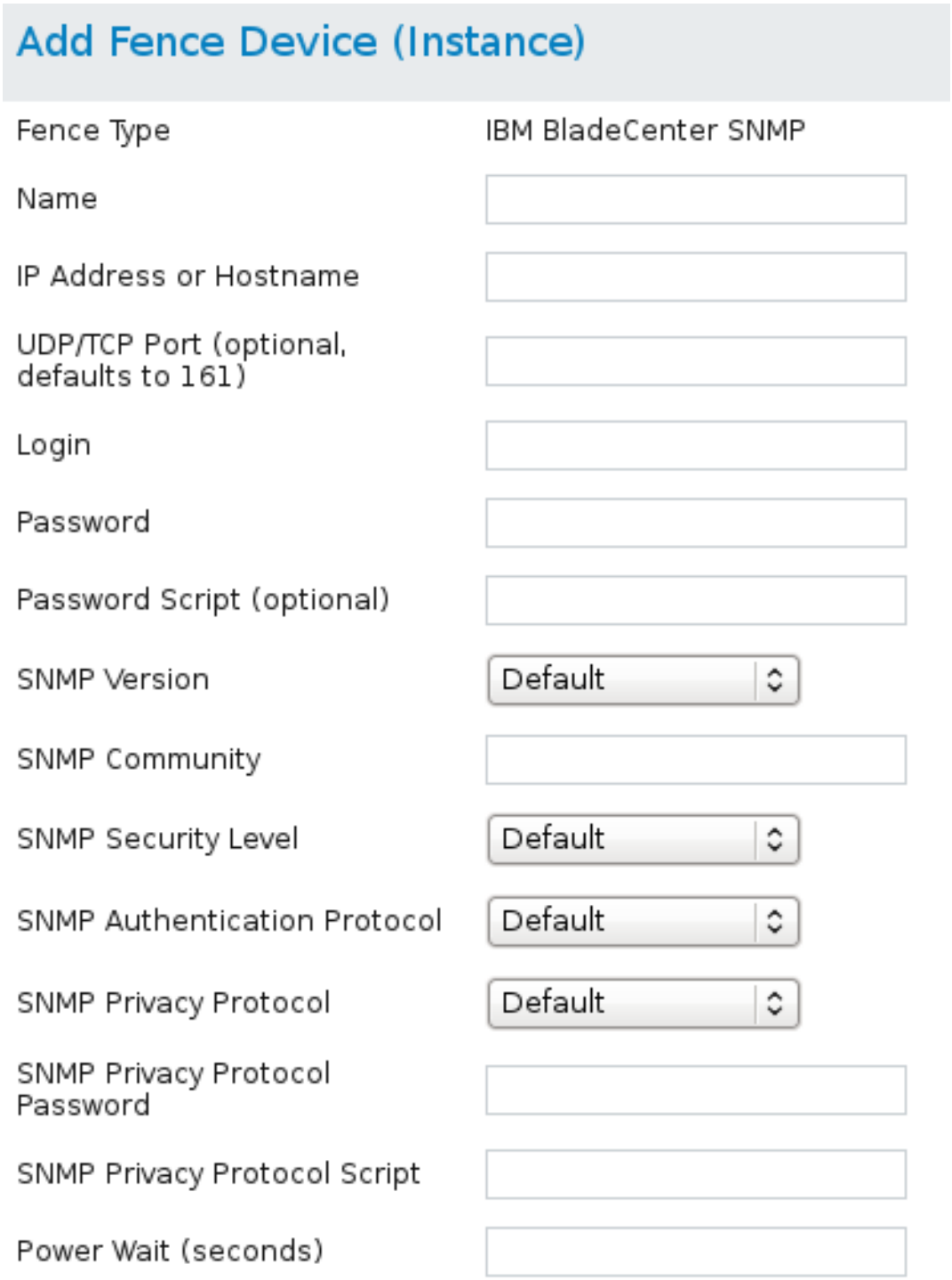


Figura 4.16. IBM BladeCenter SNMP

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo BladeCenter SNMP:

```
ccs -f cluster.conf --addfencedev bladesnmp1 agent=fence_ibmblade
community=private ipaddr=192.168.0.1 login=root \n passwd=password123
snmp_priv_passwd=snmpasswd123 power_wait=60
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_ibmblade`** :

```
 <fencedevices>
  <fencedevice agent="fence_ibmblade" community="private"
ipaddr="192.168.0.1" login="root" name="bladesnmp1" \n
```

```
passwd="password123" power_wait="60" snmp_priv_passwd="snmpasswd123"
udpport="161"/>
 </fencedevices>
```

4.18. IBM IPDU

La Tabla 4.19, “IBM iPDU (Red Hat Enterprise Linux 6.4 y posterior)” lista los parámetros de dispositivos de vallas utilizados por **fence_ipdu**, el agente de vallas para iPDU sobre dispositivos SNMP.

Tabla 4.19. 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 daemon de vallas 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.
Inicio de sesión	**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 vallas. 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).

Campo luci	Atributo `cluster.conf`	Descripción
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.
Tiempo límite de energía (segundos	**`power_timeout`**	Número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	Número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	Número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
Número de puerto (salida)	**`port`**	El número de conexión física o nombre de la máquina virtual.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.17, “IBM iPDU” muestra la pantalla de configuración para adicionar un dispositivo de vallas IBM iPDU.

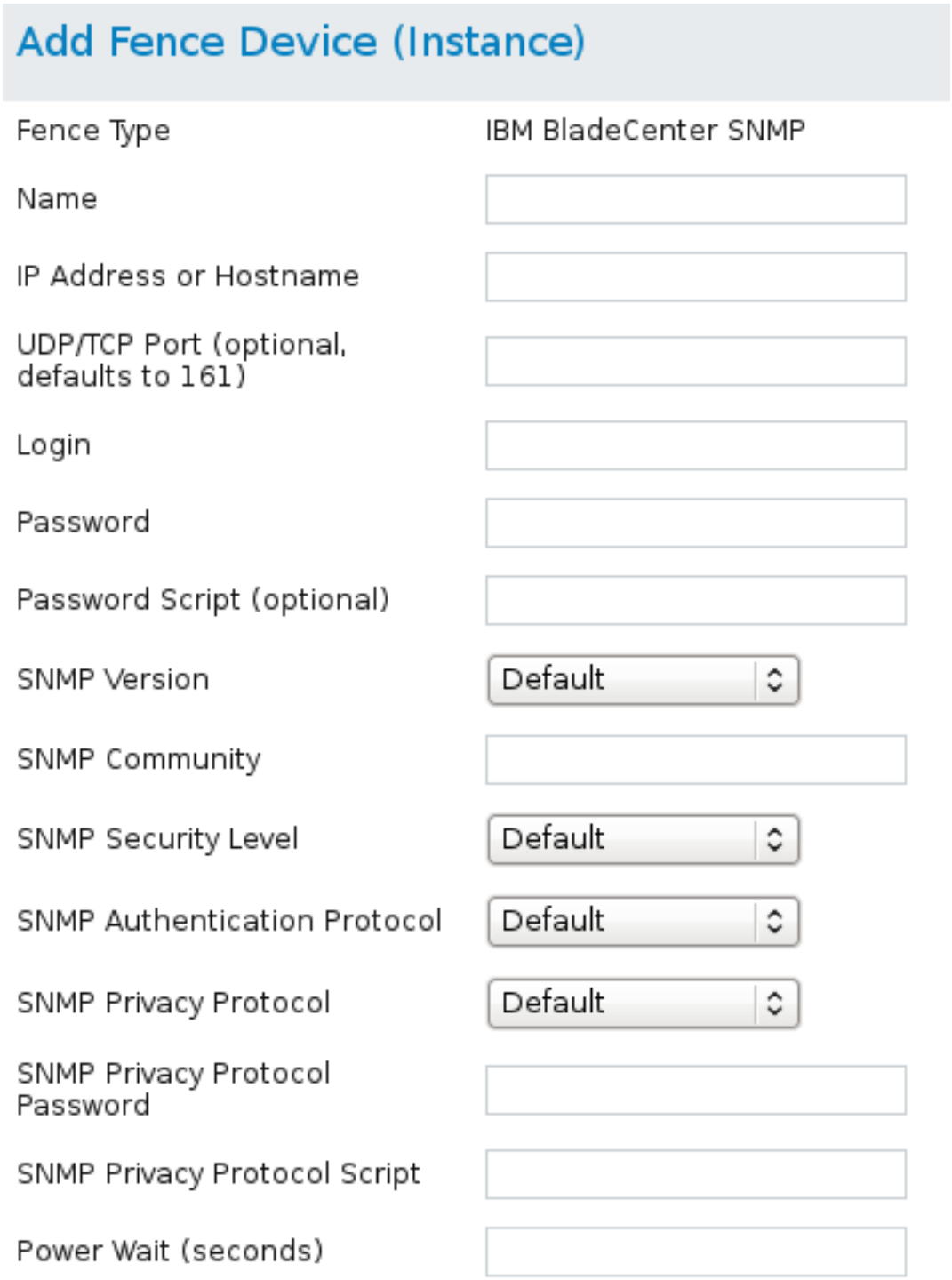


Figura 4.17. IBM iPDU

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo IBM iPDU:

```
ccs -f cluster.conf --addfencedev ipdutest1 agent=fence_ipdu
community=ipdusnmpcom ipaddr=192.168.0.1 login=root \n passwd=password123
snmp_priv_passwd=snmpasswd123 power_wait=60 snmp_priv_prot=AES udpport=111
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_ipdu`** :

```
 <fencedevices>
  <fencedevice agent="fence_ipdu" community="ipdusnmpcom"
ipaddr="ipduhost" login="root" name="ipdutest1" \n   passwd="password123"
```

```
power_wait="60" snmp_priv_passwd="ipduprivprotpasswd" snmp_priv_prot="AES"
\n   udpport="111"/>
 </fencedevices>
```

4.19. IF-MIB

La Tabla 4.20, “IF MIB” lista los parámetros de dispsitivos utilizados por **fence_ifmib**, el agente de vallas para dispositivos IF-MIB.

Tabla 4.20. 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.
Inicio de sesión	**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 vallas. 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).

Campo luci	Atributo `cluster.conf`	Descripción
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`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo de espera (segundos	**`power_timeout`**	Número de segundos de espera antes de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	El número de conexión física o nombre de la máquina virtual.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.18, “IF-MIB” muestra la pantalla de configuración para adicionar un dispositivo de vallas IF-MIB.

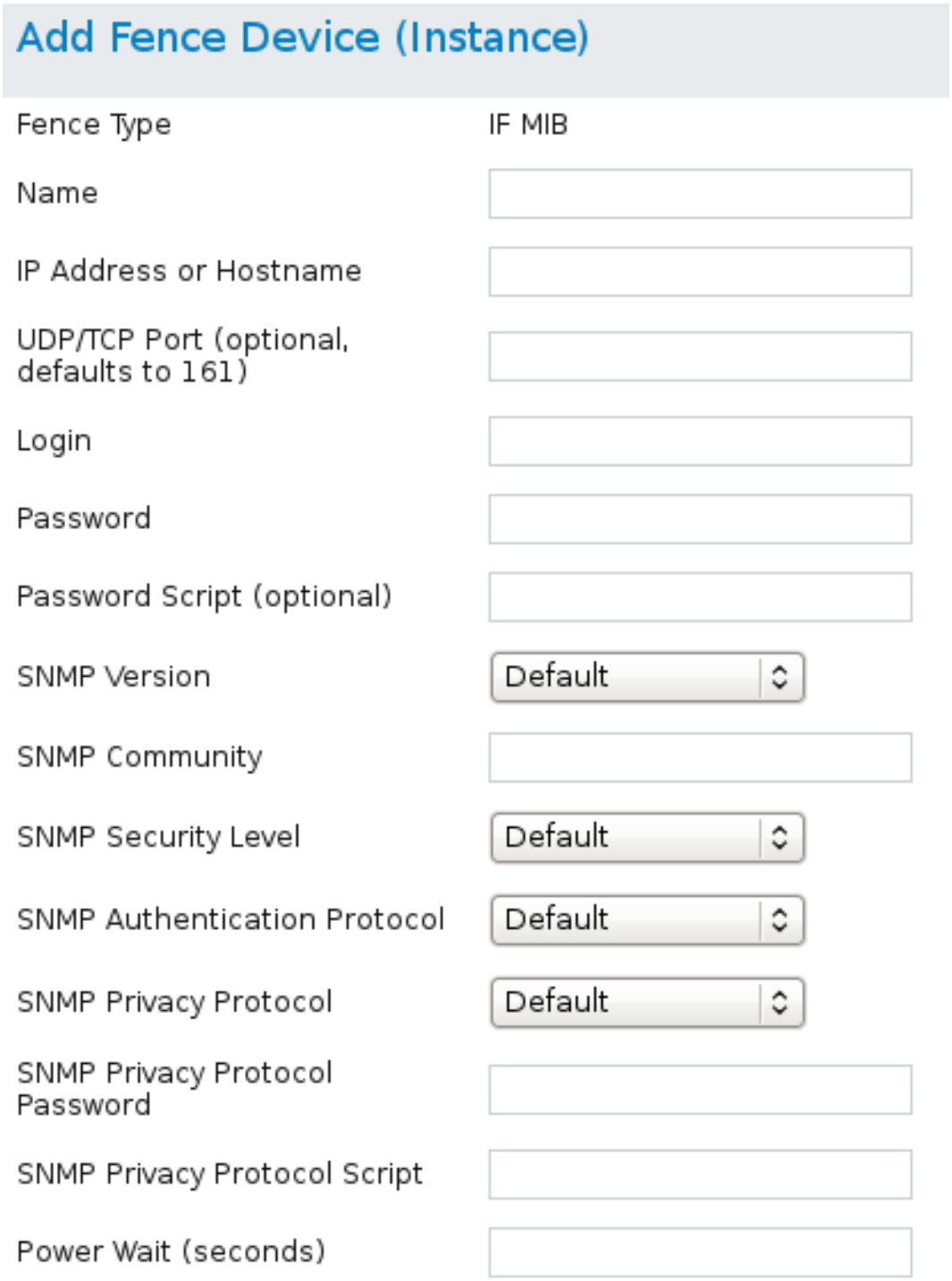


Figura 4.18. IF-MIB

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo IF-MIB.

```
ccs -f cluster.conf --addfencedev ifmib1 agent=fence_ifmib
community=private ipaddr=192.168.0.1 login=root \n passwd=password123
snmp_priv_passwd=snmpasswd123 power_wait=60 udpport=161
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_ifmib`** :

```
 <fencedevices>
  <fencedevice agent="fence_ifmib" community="private"
```

```
ipaddr="192.168.0.1" login="root" name="ifmib1" \n   passwd="password123"
power_wait="60" snmp_priv_passwd="snmpasswd123" udpport="161"/>
 </fencedevices>
```

4.20. INTEL MODULAR

La Tabla 4.21, “Intel Modular” lista los parámetros de dispositivos utilizados por **`fence_intelmodular`**, el agente de vallas para Intel Modular.

Tabla 4.21. 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.
Puerto UDP/TCP (opcional)	**`udpport`**	El puerto UDP/TCP a usar para la conexión con el dispositivo, el valor predeterminado es 161.
Inicio de sesión	**`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 vallas. 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).

Campo luci	Atributo `cluster.conf`	Descripción
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`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera antes de la prueba para un cambio de estatus después de emitir un encendido o un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	El número de conexión física o nombre de la máquina virtual.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.19, “Intel Modular” muestra la pantalla de configuración para adicionar un dispositivo de vallas Intel Modular.

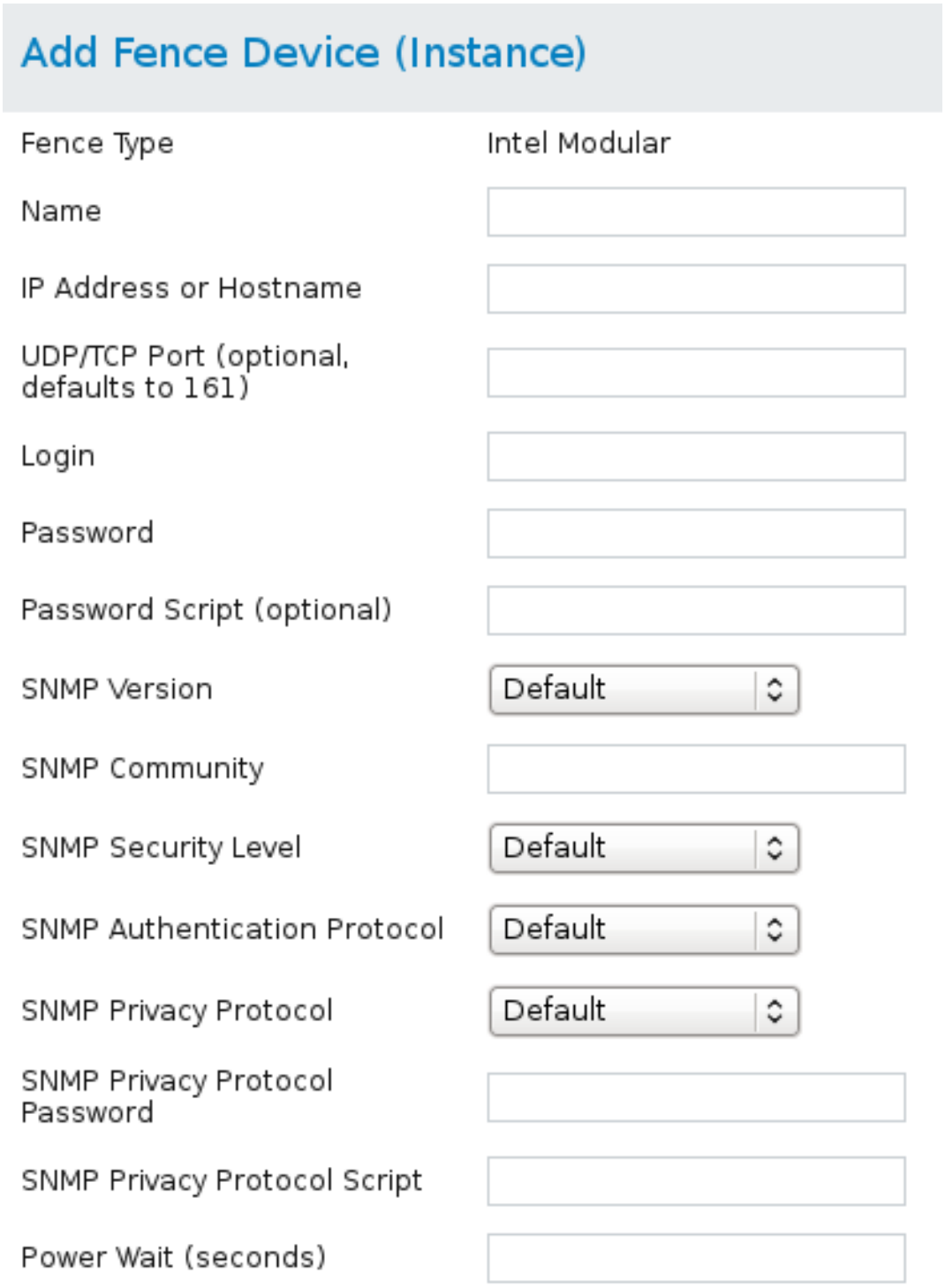


Figura 4.19. Intel Modular

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo Intel Modular:

```
ccs -f cluster.conf --addfencedev intelmodular1 agent=fence_intelmodular
community=private ipaddr=192.168.0.1 login=root \n passwd=password123
snmp_priv_passwd=snmpasswd123 power_wait=60 udpport=161
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_intelmodular`** :

```
 <fencedevices>
  <fencedevice agent="fence_intelmodular" community="private"
ipaddr="192.168.0.1" login="root" name="intelmodular1" \n
```

```
passwd="password123" power_wait="60" snmp_priv_passwd="snmpasswd123"
udpport="161"/>
 </fencedevices>
```

4.21. IPMI SOBRE LAN

Los agentes de dispositivos de vallas para IPMI sobre LAN (**fence_ipmilan**,) Dell iDRAC (**fence_idrac**), IBM Integrated Management Module (**fence_imm**), dispositivos HP iLO3 (**fence_ilo3**), y dispositivos HP iLO4 **fence_ilo4**) comparten la misma implementación. La Tabla 4.22, “LAN IPMI (Interfaz de administración de plataforma inteligente), Dell iDrac, IBM Integrated Management Module, HPiLO3, HPiLO4.” lista los parámetros de dispositivos de vallas utilizados por estos agentes.

Tabla 4.22. LAN IPMI (Interfaz de administración de plataforma inteligente), Dell iDrac, IBM Integrated Management Module, HPiLO3, HPiLO4.

Campo luci	Atributo cluster.conf	Descripción
Nombre	**name**	Un nombre para el dispositivo de vallas conectado al clúster.
Dirección IP o nombre de host	**ipaddr**	La dirección IP o nombre de host asignado al dispositivo.
Inicio de sesión	**login**	El nombre de inicio del usuario que puede emitir comandos de apagado y encendido al puerto determinado.
Contraseña	**passwd**	La contraseña para autenticar la conexión al puerto.
Script de contraseña (opcional)	**passwd_script**	El script que proporciona una contraseña para acceder al dispositivo de vallas. Su uso remplaza el parámetro de **Contraseña**.
Tipo de autenticación	**auth**	Tipo de autenticación: **none**, **password**, o **md5**.
Usar Lanplus	**lanplus**	**True** o **1**. Si está en blanco, entonces el valor es **False**. Se recomienda activar Lanplus para mejorar la seguridad de su conexión si su hardware lo soporta.
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.
Tiempo límite de IPMI	**timeout**	Tiempo límite en segundos para una operación IPMI.

Campo luci	Atributo `cluster.conf`	Descripción
Power wait (segundos)	**`power_wait`**	El número de segundos de espera después de emitir un apagado o un comando de apagado. El valor predeterminado es 2 segundos para **`fence_ipmilan`**, **`fence_idrac`**, **`fence_imm`**, y **`fence_ilo4`**. El valor predeterminado es 4 segundos para **`fence_ilo3`**.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.20, “IPMI sobre LAN” muestra la pantalla de configuración para adicionar un dispositivo de vallas IPMI.

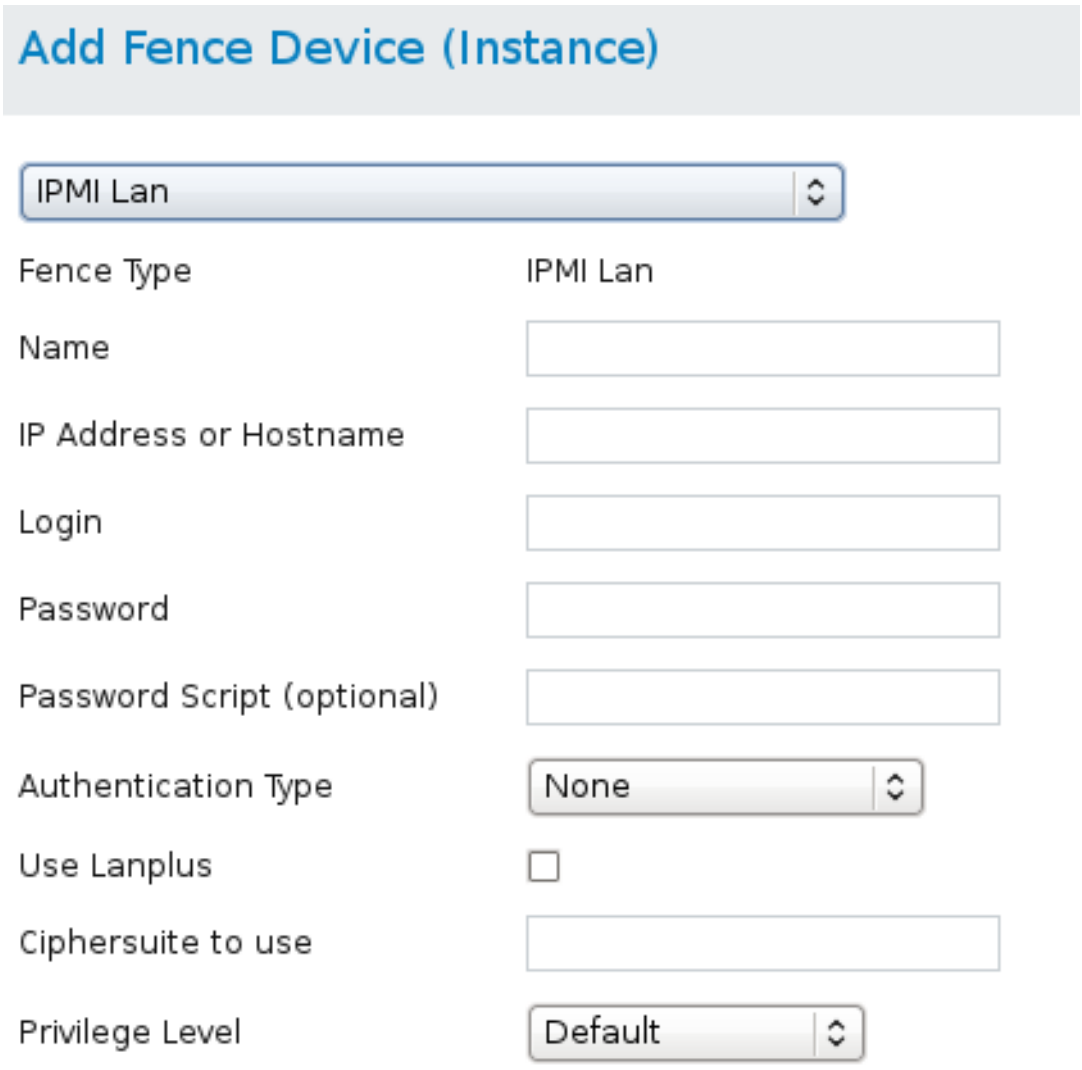


Figura 4.20. IPMI sobre LAN

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo IPMI sobre LAN:

```
ccs -f cluster.conf --addfencedev ipmitest1 agent=fence_ipmilan
auth=password cipher=3 ipaddr=192.168.0.1 \n lanplus=on login=root
passwd=password123
```

La siguiente es la entrada **cluster.conf** para el dispositivo **fence_ipmilan** :

```
 <fencedevices>
  <fencedevice agent="fence_ipmilan" auth="password" cipher="3"
ipaddr="192.168.0.1" lanplus="on" login="root" \n   name="ipmitest1"
passwd="password123"/>
 </fencedevices>
```

4.22. RHEV-M REST API

La Tabla 4.23, “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 4.23. 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 vallas 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.
Inicio de sesión	**login**	El nombre de usuario utilizado para acceder al 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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Usa SSL	**ssl**	Usa las conexiones SSL para comunicarse con el dispositivo.
Power wait (segundos)	**power_wait**	El número de segundos de espera después de expedir un comando de apagado o encendido.

Campo luci	Atributo `cluster.conf`	Descripción
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera después de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir un comando. El valor predeterminado es 3.
El tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
El número de puerto (salida)	**`port`**	El número de conexión física o nombre de la máquina virtual.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.21, “RHEV-M REST API” muestra la pantalla de configuración para agregar un dispositivo RHEV-M REST API.

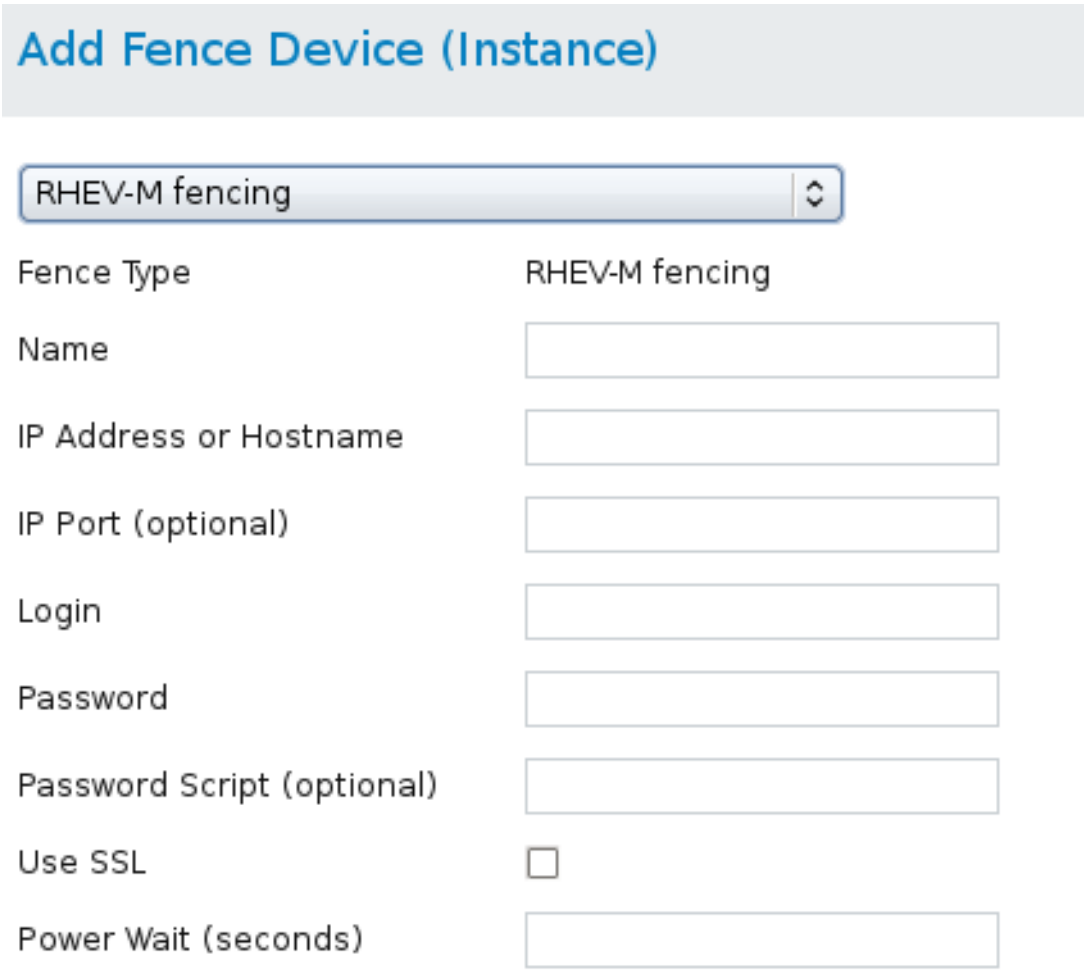


Figura 4.21. RHEV-M REST API

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo RHEV-M REST API:

```
ccs -f cluster.conf --addfencedev rhevmtest1 agent=fence_rhevm
ipaddr=192.168.0.1 login=root passwd=password123 \n power_wait=60 ssl=on
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_rhevm`** :

```
 <fencedevices>
  <fencedevice agent="fence_rhevm" ipaddr="192.168.0.1" login="root"
name="rhevmtest1" passwd="password123" \n   power_wait="60" ssl="on"/>
 </fencedevices>
```

4.23. RESERVACIONES PERSISTENTES SCSI

La Tabla 4.24, “Cercado de reservaciones SCSI ” lista los parámetros de dispositivos de vallas utilizados por **`fence_scsi`**, el agente de vallas para reservaciones persistentes SCSI.

NOTA

El uso de reservaciones SCSI persistentes como un método de vallas 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.

Se recomienda que los dispositivos utilizados para los volúmenes de clúster estén en el formato **/dev/disk/by-id/***xxx*. Los dispositivos especificados en este formato son consistentes dentro de todos los nodos y apuntarán al mismo disco, a menos que se especifique en un formato tal como **/dev/sda**, el cual apunta a diferentes discos de máquina a máquina tras reinicios.

Tabla 4.24. Cercado de reservaciones SCSI

Campo luci	Atributo `cluster.conf`	Descripción
Nombre	**name**	Un nombre para el dispositivo de vallas SCSI.
Unfencing	La sección **unfence** del archivo de configuración	Cuando está activado, asegura que el nodo cercado no se reactive sino hasta un nuevo arranque del nodo. Esto se requiere para los métodos de vallas sin energía: cercado de almacenamiento y SAN. Para configurar un dispositivo que requiera sin cercado(unfencing), primero debe detener el clúster y toda la configuración, incluidos los dispositivos y debe agregar sin cercado antes de iniciar el clúster. Para obtener más información, consulte la página de manual **fence_node**(8). Para información sobre cómo configurar sin cercado, consulte:
Nombre de nodo	**nodename**	El nombre de nodo que sirve para generar el valor de llave para la operación actual.
Llave para la acción actual	**key**	(Sobrescribe el nombre de nodo) Llave a usar para la operación actual. Esta llave debe ser única para un nodo. Para una acción "on" (encendido), la llave especifica la clave a usar para registrar el nodo local. Para la acción "off" (apagado), la llave especifica la clave que va a ser eliminada del/los dispositivo(s).
Retraso (opcional)	**delay**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.

La Figura 4.22, “Cercado SCSI” muestra la pantalla de configuración para adicionar un dispositivo de vallas SCSI.

Figura 4.22. Cercado SCSI

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo de vallas SCSI:

```
ccs -f cluster.conf --addfencedev scsifencetest1 agent=fence_scsi
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_scsi`** :

```
<fencedevices>
 <<fencedevice agent="fence_scsi" name="scsifencetest1"/>
</fencedevices>
```

4.24. VMWARE SOBRE SOAP API

La Tabla 4.25, “vallas de VMware (Interfaz SOAP) (Red Hat Enterprise Linux 6.2 y posterior)”lista los parámetros de dispositivos de vallas utilizados por **`fence_vmware_soap`**, el agente de vallas para VMWare en SOAP API.

Tabla 4.25. 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 vallas Fence virt.
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 el dispositivo. El puerto predeterminado es 80 o443 si selecciona **`Usar SSH`**
Inicio de sesión	**`login`**	El nombre de usuario utilizado para acceder el dispositivo.
Contraseña	**`passwd`**	La contraseña utilizada para autenticar la conexión al dispositivo.

Campo luci	Atributo `cluster.conf`	Descripción
Script de contraseña (opcional)	**`passwd_script`**	El script que proporciona una contraseña para acceder al dispositivo de vallas. Su uso remplaza el parámetro de **Contraseña**.
Power wait (segundos)	**`power_wait`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera después de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
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.
Retraso (opcional)	**`delay`**	El número de segundos de espera antes del inicio de cercado. El valor predeterminado es 0.
Usa SSL	**`ssl`**	Usa las conexiones SSL para comunicarse con el dispositivo.

La Figura 4.23, “VMWare sobre cercado SOAP” muestra la pantalla de configuración para adicionar un dispositivo SOAP.

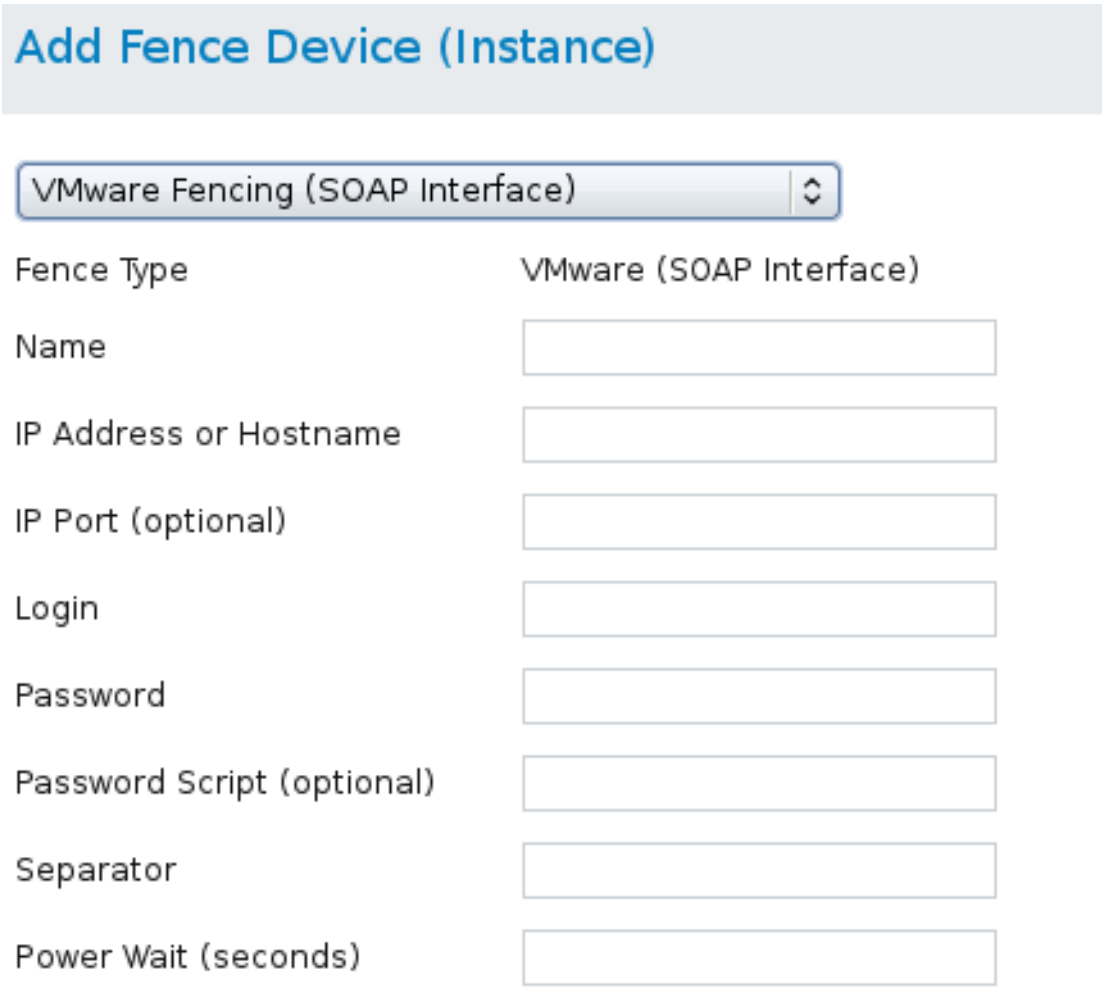


Figura 4.23. VMWare sobre cercado SOAP

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo de vallas SOAP:

```
ccs -f cluster.conf --addfencedev vmwaresoaptest1 agent=fence_vmware_soap
login=root passwd=password123 power_wait=60 \n separator=,
```

La siguiente es la entrada **`cluster.conf`** para el dispositivo **`fence_vmware_soap`** :

```
 <fencedevices>
  <fencedevice agent="fence_vmware_soap" ipaddr="192.168.0.1" login="root"
name="vmwaresoaptest1" passwd="password123" \n   power_wait="60"
separator="."/>
 </fencedevices>
```

4.25. WTI POWER SWITCH

La Tabla 4.26, “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 4.26. 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.
Inicio de sesión	**`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 vallas. Su uso remplaza el parámetro de **Contraseña**.
Forzar el indicador de comandos	**`cmd_prompt`**	El indicador de comandos a usar. El valor predeterminado es ['RSM>', '>MPC', 'IPS>', 'TPS>', 'NBB>', 'NPS>', 'VMR>']
Power wait (segundos)	**`power_wait`**	El número de segundos de espera después de expedir un comando de apagado o encendido.
Tiempo límite de energía (segundos)	**`power_timeout`**	El número de segundos de espera después de la prueba para un cambio de estatus después de expedir un comando de encendido. El valor predeterminado es 20.
Tiempo límite de shell (segundos)	**`shell_timeout`**	El número de segundos de espera por un indicador de comandos después de emitir el comando. El valor predeterminado es 3.
Tiempo límite de inicio de sesión (segundos)	**`login_timeout`**	El número de segundos de espera por un indicador de comandos después de iniciar sesión. El valor predeterminado es 5.
El número de intentos de encendido	**`retry_on`**	El número intentos de encendido. El valor predeterminado es 1.
Usa SSH	**`secure`**	Indica que el sistema utilizará SSH para acceder al dispositivo. Cuando use SSH, debe especificar ya sea la contraseña, el script de la contraseña o un archivo de identidad.

Campo luci	Atributo `cluster.conf`	Descripción
Opciones de SSH	**`ssh_options`**	Opciones SSH a usar. El valor predeterminado es **`-1 -c blowfish`**.
Ruta al archivo de identidad SSH	**`identity_file`**	El archivo de identidad para SSH.
Puerto	**`port`**	El número de conexión física o nombre de la máquina virtual.

La Figura 4.24, “Cercado WTI” muestra la pantalla de configuración para adicionar un dispositivo de vallas WTI.

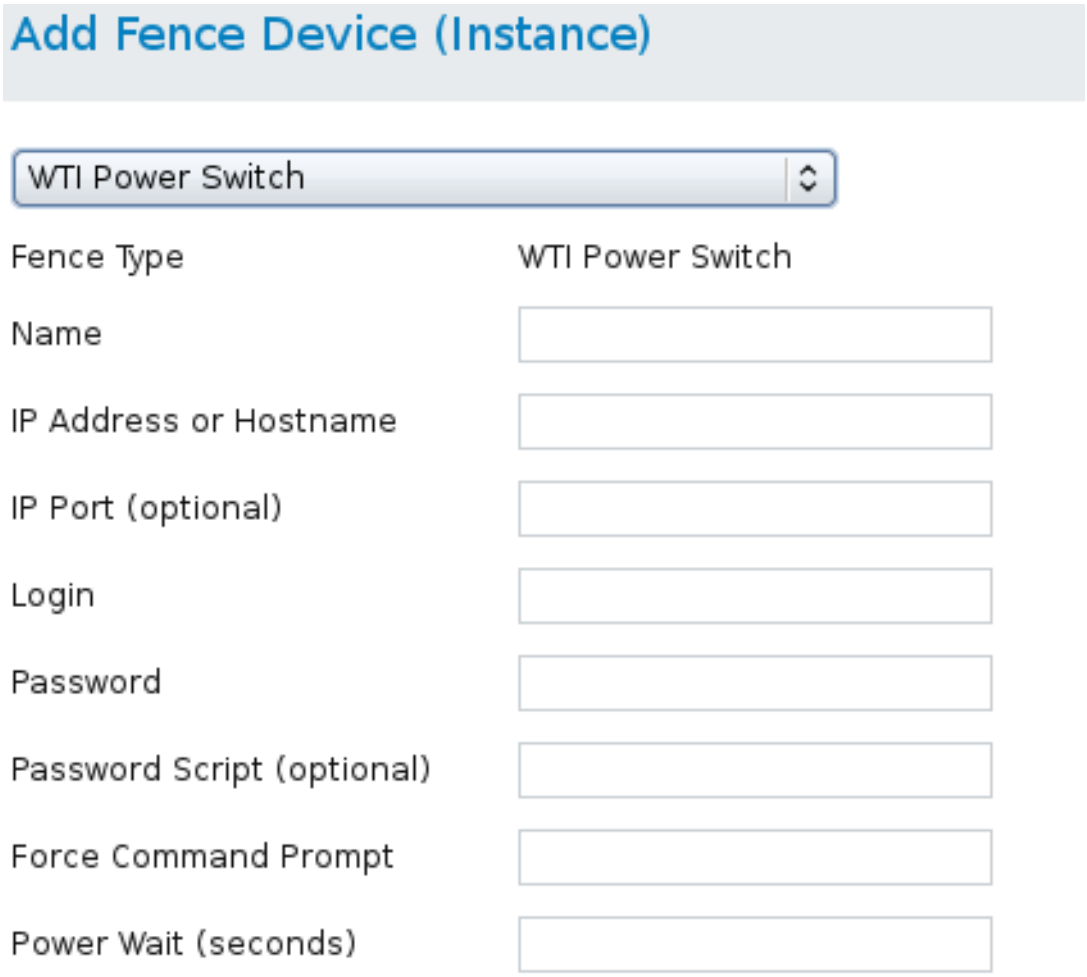


Figura 4.24. Cercado WTI

El siguiente comando crea una instancia de dispositivo de vallas para un dispositivo de vallas WTI:

```
ccs -f cluster.conf --addfencedev wtipwrsw1 agent=fence_wti
cmd_prompt=VMR> login=root passwd=password123 \n power_wait=60
```

La siguiente es la entrada **cluster.conf** para el dispositivo **fence_wti** :

```
 <fencedevices>
  <fencedevice agent="fence_wti" cmd_prompt="VMR&gt;" ipaddr="192.168.0.1"
login="root" name="wtipwrsw1" \n   passwd="password123" power_wait="60"/>
 </fencedevices>
```

APÉNDICE A. HISTORIA DE REVISIONES

Revisión 1-15.2 **Wed Feb 11 2015** **Gladys Guerrero-Lozano**
translated

Revisión 1-15.1 **Wed Feb 11 2015** **Gladys Guerrero-Lozano**
Los archivos de traducción sincronizados con fuentes XML 1-15

Revisión 1-15 **Tue Dec 16 2014** **Steven Levine**
Updating to implement sort_order on the RHEL 6 splash page.

Revisión 1-13 **Wed Oct 8 2014** **Steven Levine**
Version for 6.6 GA Release

Revisión 1-11 **Thu Aug 7 2014** **Steven Levine**
Lanzamiento para Beta de Red Hat Enterprise Linux 6.6

Revisión 1-10 **Thu Jul 31 2014** **Steven Levine**
Resuelve: #856311
Documenta la página de manual fence_check.

Resuelve: #1104910
Actualiza las tablas de parámetros de vallas con parámetros de dispositivos de vallas.

Revisión 1-9 **Wed Nov 20 2013** **John Ha**
Lanzamiento para disponibilidad general de Red Hat Enterprise Linux 6.5

Revisión 1-4 **Mon Nov 28 2012** **John Ha**
Lanzamiento para Beta de Red Hat Enterprise Linux 6.5

Revisión 1-2 **Mon Nov 28 2012** **John Ha**
Lanzamiento para Beta de Red Hat Enterprise Linux 6.4

ÍNDICE

A

C

D