Red Hat Enterprise Linux 6

Amministrazione del cluster

Configurazione e gestione di High Availability Add-On

Last Updated: 2017-10-12

Red Hat Enterprise Linux 6 Amministrazione del cluster

Configurazione e gestione di High Availability Add-On

Red Hat Engineering Content Services
docs-need-a-fix@redhat.com

Nota Legale

Sommario

Configurazione e gestione di High Availability Add-On Questa guida descrive le configurazione e la gestione di High Availability Add-On per Red Hat Enterprise Linux 6.

Indice

INTRODUZIONE

Questo documento fornisce le informazioni relative all'installazione, configurazione e gestione dei componenti di Red Hat High Availability Add-On. Questi componenti permetteranno di collegarvi ad un gruppo di computer (chiamati *nodi* o *membri*) che operano tra loro come un cluster. In questo documento la parola *cluster* viene usata come riferimento per un gruppo di computer in esecuzione con il Red Hat High Availability Add-On.

È rivolto a coloro che possiedono una conoscenza avanzata di Red Hat Enterprise Linux e dei concetti di cluster, storage, e server computing.

Per maggiori informazioni su Red Hat Enterprise Linux 6 consultate le seguenti risorse:

- *Red Hat Enterprise Linux Installation Guide*— Fornisce le informazioni relative all'installazione di Red Hat Enterprise Linux 6.
- *Red Hat Enterprise Linux Deployment Guide* — Fornisce le informazioni relative all'impiego, configurazione ed amministrazione di Red Hat Enterprise Linux 6.

Per maggiori informazioni sull'High Availability Add-On e sui prodotti relativi per Red Hat Enterprise Linux 6 consultate le seguenti risorse:

- *Panoramica High Availability Add-On* — Fornisce una panoramica dettagliata sul Red Hat High Availability Add-On.
- *Logical Volume Manager Administration* — Fornisce una descrizione sul Logical Volume Manager (LVM), e su come eseguire LVM in un ambiente clusterizzato.
- *Global File System 2: Configurazione e amministrazione* — Fornisce le informazioni relative all'installazione, configurazione e gestione del Red Hat GFS2 (Red Hat Global File System 2), incluso nel Resilient Storage Add-On.
- *DM Multipath* — Fornisce le informazioni relative all'uso del Device-Mapper Multipath di Red Hat Enterprise Linux 6.
- *Amministrazione del Load Balancer*— Fornisce le informazioni necessarie per la configurazione dei servizi e dei sistemi ad elevate prestazioni con Load Balancer Add-On, un insieme di componenti software i quali forniscono il Linux Virtual Server [LVS] per il bilanciamento del carico IP su di un set di real server.
- *Note di rilascio* — Fornisce le informazioni relative alla release corrrente dei prodotti di Red Hat.

La documentazione relativa all'High Availability Add-On ed altre documentazioni di Red Hat sono disponibili in versione HTML, PDF, e RPM sul CD di documentazione di Red Hat Enterprise Linux ed online su http://docs.redhat.com/docs/en-US/index.html.

1. COMMENTI

Se individuate degli errori di battitura in questo manuale, o se pensate di poter contribuire al suo miglioramento, contattateci subito! Inviate i vostri suggerimenti tramite Bugzilla (http://bugzilla.redhat.com/bugzilla/) nei confronti del componente **doc-Cluster_Administration**.

Assicuratevi di indicare l'identificatore del manuale:

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

Indicando l'identificatore del manuale noi sapremo esattamente di quale versione siete in possesso.

Se inviate un suggerimento per contribuire al miglioramento della guida, cercate di essere il più specifici possibile. Se avete individuato un errore, indicate il numero della sezione e alcune righe di testo in modo da agevolare la ricerca dell'errore.

CAPITOLO 1. PANORAMICA SULLA GESTIONE E SULLA CONFIGURAZIONE DI RED HAT HIGH AVAILABILITY ADD-ON

Red Hat High Availability Add-On permette all'utente di collegarsi ad un gruppo di computer (chiamati *nodi* o *membri*) e lavorare insieme come un cluster. Sarà possibile usare il Red Hat High Availability Add-On per soddisfare i requisiti del cluster (per esempio per l'impostazione di un cluster per la condivisione dei file su di un file system GFS2 o per l'impostazione di un failover del servizio).

NOTA

Per informazioni sulle migliori implementazioni e sugli aggiornamenti dei cluster di Red Hat Enterprise Linux utilizzando High Availability Add-On e Red Hat Global File System 2 (GFS2) consultate l'articolo "Red Hat Enterprise Linux Cluster, High Availability, e GFS Deployment Best Practices" sul Portale clienti di Red Hat . https://access.redhat.com/kb/docs/DOC-40821.

Questo capitolo fornisce un sommario sulla documentazione degli aggiornamenti e sulle funzioni aggiunte al Red Hat High Availability Add-On dalla release iniziale di Red Hat Enterprise Linux 6, seguito da una panoramica sulla configurazione e gestione di Red Hat High Availability Add-On.

1.1. FUNZIONI NUOVE E MODIFICATE

Questa sezione riporta le funzioni nuove e quelle modificate di Red Hat High Availability Add-On incluse dalla release iniziale di Red Hat Enterprise Linux 6.

1.1.1. Funzioni nuove e modificate di Red Hat Enterprise Linux 6.1

Red Hat Enterprise Linux 6.1 include le seguenti modifiche e gli aggiornamenti relativi alla documentazione ed alle funzioni.

- Con Red Hat Enterprise Linux 6.1 e versioni più recenti il Red Hat High Availability Add-On fornisce il supporto per SNMP trap. Per informazioni su come configurare SNMP trap tramite Red Hat High Availability Add-On consultare Capitolo 10, *Configurazione SNMP con Red Hat High Availability Add-On*.
- Con Red Hat Enterprise Linux 6.1 e versioni più recenti il Red Hat High Availability Add-On fornisce il supporto del comando per la configurazione del cluster **ccs**. Per informazioni sul comando **ccs** consultare Capitolo 5, *Configurazione di Red Hat High Availability Add-On con il comando **ccs*** e Capitolo 6, *Gestione di Red Hat High Availability Add-On con **ccs***.
- La documentazione per la configurazione e gestione di Red Hat High Availability Add-On tramite Conga è stata aggiornata ed ora riflette il supporto delle funzioni e le schermate di Conga.
- Con Red Hat Enterprise Linux 6.1 e versioni più recenti l'uso di **ricci** richiederà l'utilizzo di una password se si inoltrerà per la prima volta la configurazione del cluster aggiornata da un qualsiasi nodo. Per informazioni su **ricci** consultare Sezione 2.13, «Considerazioni su **ricci**».
- È possibile ora specificare una politica *Restart-Disable*. Con questa politica in caso di fallimento di un servizio il sistema cercherà di eseguire un riavvio, se questa operazione fallisce il servizio sarà disabilitato e non verrà spostato su alcun host presente nel cluster. Questa funzione è documentata in Sezione 3.10, «Come aggiungere un servizio ad un cluster» e Appendice B, *Parametri della risorsa HA*.

- È ora possibile configurare un albero secondario indipendente come non-critico, così facendo se la risorsa fallisce solo quella risorsa verrà disabilitata. Per informazioni su questa funzione consultare Sezione 3.10, «Come aggiungere un servizio ad un cluster» e Sezione C.4, «Ripristino fallito ed alberi secondari indipendenti».

- Questo documento include ora il nuovo capitolo Capitolo 9, *Diagnosi e correzione dei problemi presenti nel cluster*.

In aggiunta sono state apportate piccole correzioni e chiarimenti su tutto il documento.

1.1.2. Funzioni nuove e modificate di Red Hat Enterprise Linux 6.2

Red Hat Enterprise Linux 6.2 include le seguenti modifiche e gli aggiornamenti relativi alla documentazione ed alle funzioni.

- Il Red Hat Enterprise Linux fornisce un supporto per Samba clusterizzati in esecuzione con una configurazione attiva/attiva. Per maggiori informazioni sulla configurazione Samba clusterizzato consultare Capitolo 11, *Configurazione samba clusterizzato*.

- Anche se qualsiasi utente in grado di eseguire una autenticazione con il sistema che ospita **luci** può effettuare un login con lo stesso **luci**, con Red Hat Enterprise Linux 6.2 solo l'utente root del sistema che esegue **luci** potrà accedere a qualsiasi dei componenti **luci** fino a quando un amministratore (l'utente root o un utente con permessi di amministrazione) imposta i permessi necessari per l'utente in questione. Per informazioni su come impostare i permessi **luci** per gli utenti consultare Sezione 3.3, «Controllo accesso di luci».

- I nodi di un cluster possono comunicare tra loro usando un meccanismo di trasporto UDP Unicast. Per informazioni su come configurare UDP Unicast consultare Sezione 2.12, «Traffico UDP Unicast».

- È ora possibile configurare alcuni aspetti del comportamento di **luci** tramite il file **`/etc/sysconfig/luci`**. Per esempio è possibile configurare in modo specifico l'unico indirizzo IP al quale viene servito **luci**. Per informazioni su come configurare l'indirizzo IP usato per servire **luci** consultare Tabella 2.2, «Porta IP abilitata su un computer che esegue **luci**». Per informazioni sul file **`/etc/sysconfig/luci`** consultare Sezione 2.4, «Configurazione di **luci** con **`/etc/sysconfig/luci`**».

- Il comando **`ccs`** include ora l'opzione **`--lsfenceopts`**, per mezzo della quale è possibile stampare un elenco di dispositivi di fencing disponibili, e l'opzione **`--lsfenceopts`** *fence_type* usata per visualizzare i diversi tipi di fencing. Per informazioni sulle suddette opzioni consultare Sezione 5.6, «Elenco dei dispositivi di fencing ed opzioni».

- Il comando **`ccs`** include ora l'opzione **`--lsserviceopts`** per mezzo della quale è possibile stampare un elenco di servizi del cluster attualmente disponibili, e l'opzione **`--lsserviceopts`** *service_type* usata per le opzioni utilizzabili per un tipo particolare di servizio. Per maggiori informazioni consultare Sezione 5.11, «Elenco dei servizi cluster disponibili».

- Il Red Hat Enterprise Linux 6.2 fornisce supporto per il VMware (interfaccia SOAP) fence agent. Per informazioni sui parametri del dispositivo di fencing consultare Appendice A, *Parametri del dispositivo di fencing*.

- Il Red Hat Enterprise Linux 6.2 fornisce supporto per il fence agent RHEV-M REST API rispetto al RHEV 3.0 e versioni più recenti. Per informazioni sui parametri del dispositivo di fencing consultare Appendice A, *Parametri del dispositivo di fencing*.

- Con Red Hat Enterprise Linux 6.2 durante la configurazione di una macchina virtuale in un

cluster con il comando **ccs** è possibile utilizzare l'opzione **--addvm** (al posto di **addservice**). Così facendo la risorsa **vm** verrà direttamente definita nel nodo di configurazione di **rm** nel file di configurazione del cluster. Per informazioni su come configurare le risorse della macchina virtuale con il comando **ccs** consultare Sezione 5.12, «Risorse della macchina virtuale».

- Questo documento include una nuova appendice Appendice D, *Controllo risorse servizio del cluster e timeout del failover* la quale descrive il processo di monitoraggio dello stato delle risorse del cluster da perte di **rgmanager**, e la modifica dell'intervallo di controllo dello stato. Inoltre l'appendice descrive anche il parametro del servizio **__enforce_timeouts** il quale indica che un timeout di una operazione potrebbe causare il fallimento del servizio.

- Questo documento include una nuova sezione, Sezione 2.3.3, «Configurazione del firewall di iptables per abilitare i componenti del cluster». La suddetta sezione mostra come eseguire il filtro per abilitare il traffico multicast attraverso il firewall **iptables** per i diversi componenti del cluster.

In aggiunta sono state apportate piccole correzioni e chiarimenti su tutto il documento.

1.1.3. Funzioni nuove e modificate di Red Hat Enterprise Linux 6.3

Red Hat Enterprise Linux 6.3 include le seguenti modifiche e gli aggiornamenti relativi alla documentazione ed alle funzioni.

- Il Red Hat Enterprise Linux 6.3 fornisce il supporto per l'agente delle risorse **condor**. Per informazioni sui parametri delle risorse HA consultare Appendice B, *Parametri della risorsa HA*.

- Questo documento include ora una nuova appendice Appendice F, *High Availability LVM (HA-LVM)*.

- Le informazioni presenti in questo documento indicano le modifiche relative alla configurazione che necessitano di un riavvio del cluster. Per un sommario di queste modifiche consultare Sezione 9.1, «Le modifiche alla configurazione non vengono implementate».

- Questa documentazione riporta ora un timeout di inattività per **luci** con il quale dopo 15 minuti di inattività l'utente verrà espulso. Per informazioni su come avviare **luci** consultare Sezione 3.2, «Avvio di **luci**».

- Il dispositivo di fencing **fence_ipmilan** supporta il parametro privilege level. Per informazioni sui parametri del dispositivo di fencing consultare Appendice A, *Parametri del dispositivo di fencing*.

- Questo documento include ora una nuova sezione Sezione 2.14, «Configurazione di macchine virtuali in un ambiente clusterizzato».

- Questo documento include ora una nuova sezione Sezione 4.6, «Backup e ripristino della configurazione di luci».

- Questo documento include ora una nuova sezione Sezione 9.4, «Arresti inaspettati del demone del cluster».

- Questo documento fornisce le informazioni sull'impostazione delle opzioni di debug in Sezione 5.14.4, «Registrazione», Sezione 7.7, «Configurazione delle opzioni di debug», e Sezione 9.13, «La registrazione del Debug per il Distributed Lock Manager (DLM) deve essere abilitata».

- Con Red Hat Enterprise Linux 6.3, l'utente root o l'utente con permessi amministrativi per **luci**, è in grado di utilizzare l'interfaccia **luci** per aggiungere gli utenti al sistema come descritto in Sezione 3.3, «Controllo accesso di luci».

- Con Red Hat Enterprise Linux 6.3 il comando **ccs** convalida la configurazione in base allo schema **/usr/share/cluster/cluster.rng** sul nodo specificato con l'opzione **-h**. In precedenza il comando **ccs** utilizzava sempre lo schema disponibile con il comando **ccs**, **/usr/share/ccs/cluster.rng** sul sistema locale. Per informazioni sulla convalida della configurazione consultare Sezione 5.1.6, «Convalida della configurazione»

- Le tabelle che descrivono i parametri del dispositivo di fencing in Appendice A, *Parametri del dispositivo di fencing* e le tabelle che descrivono i parametri delle risorse HA in Appendice B, *Parametri della risorsa HA*, includono ora i nomi dei suddetti parametri come riportato nel file **cluster.conf**.

In aggiunta sono state apportate piccole correzioni e chiarimenti su tutto il documento.

1.1.4. Funzioni nuove e modificate di Red Hat Enterprise Linux 6.4

Red Hat Enterprise Linux 6.4 include le seguenti modifiche e gli aggiornamenti relativi alla documentazione ed alle funzioni.

- Il Red Hat Enterprise Linux 6.4 rende disponibile il supporto per Eaton Network Power Controller (Interfaccia SNMP) fence agent, HP BladeSystem fence agent, e the IBM iPDU. Per informazioni sui parametri del dispositivo di fencing consultare Appendice A, *Parametri del dispositivo di fencing*.

- Appendice B, *Parametri della risorsa HA* ora fornisce una descrizione dei NFS Server resource agent.

- Con Red Hat Enterprise Linux 6.4, l'utente root o l'utente con permessi amministrativi per **luci**, è in grado di utilizzare l'interfaccia **luci** per cancellare gli utenti dal sistema come descritto in Sezione 3.3, «Controllo accesso di luci».

- Appendice B, *Parametri della risorsa HA* fornisce una descrizione del nuovo parametro **nfsrestart** per le risorse Filesystem e GFS2 HA.

- Questo documento include ora una nuova sezione Sezione 5.1.5, «Comandi che sovrascrivono le impostazioni precedenti».

- Sezione 2.3, «Abilitare le porte IP» include ora le informazioni sul filtraggio del firewall **iptables** per **igmp**.

- L' IPMI LA fence agent supporta ora un parametro per la configurazione del livello di privilegi sul dispositivo IPMI come riportato in Appendice A, *Parametri del dispositivo di fencing*.

- In aggiunta alla modalità bonding 1 di Ethernet, sono ora supportate anche le modalità 0 e 2 per le comunicazioni tra i nodi presenti in un cluster. L'avvertimento relativo presente sul Troubleshooting riporta le informazioni sul supporto delle nuove modalità.

- I dispositivi di rete contrassegnati con VLAN sono ora supportati per una comunicazione heartbeat del cluster. L'avviso relativo alla mancanza di supporto dei suddetti dispositivi è stato rimosso da questa documentazione.

- Il Red Hat High Availability Add-On supporta ora la configurazione del protocollo ring ridondante. Per informazioni generali su come usare questa funzione e configurare il file **cluster.conf**

consultare Sezione 7.6, «Configurazione Protocollo ring ridondante». Per informazioni su come configurare il protocollo ring ridondante con **luci** consultare Sezione 3.5.4, «Configurazione Protocollo ring ridondante». Per le informazioni utili per una configurazione usando **ccs** consultare Sezione 5.14.5, «Configurazione Protocollo ring ridondante».

In aggiunta sono state apportate piccole correzioni e chiarimenti su tutto il documento.

1.2. CONCETTI DI BASE PER LA CONFIGURAZIONE

Per impostare un cluster collegare i nodi con l'hardware specifico e configurarli in un ambiente cluster. La configurazione e gestione di Red Hat High Availability Add-On consiste nelle seguenti fasi:

1. Impostazione dell'hardware. Consultare la Sezione 1.3, «Impostazione dell'hardware».
2. Installazione del software di Red Hat High Availability Add-On. Consultare la Sezione 1.4, «Installazione software di Red Hat High Availability Add-On».
3. Configurazione del software di Red Hat High Availability Add-On. Consultare la Sezione 1.5, «Configurazione del software di Red Hat High Availability Add-On».

1.3. IMPOSTAZIONE DELL'HARDWARE

L'impostazione dell'hardware consiste nel collegare i nodi del cluster con un altro hardware necessario per l'esecuzione di Red Hat High Availability Add-On. La quantità ed il tipo di hardware varia in base allo scopo ed ai requisiti del cluster. Generalmente un cluster di livello enterprise ha bisogno del seguente tipo di hardware (consultare la Figura 1.1, «Panoramica sull'hardware di Red Hat High Availability Add-On»). Per considerazioni relative all'hardware ed altre problematiche riguardanti la configurazione del cluster consultare il Capitolo 2, *Prima di configurare Red Hat High Availability Add-On* o un rappresentante Red Hat autorizzato.

- Nodi del cluster — Computer in grado di eseguire un software Red Hat Enterprise Linux con almeno 1GB di RAM.
- Hub o interruttore Ethernet per la rete pubblica — Necessario per un accesso client al cluster.
- Hub o interruttore Ethernet per la rete privata — Necessario per la comunicazione tra i nodi del cluster ed un altro hardware del cluster come ad esempio gli interruttori di alimentazione di rete e gli interruttori del Fibre Channel.
- Interruttore di alimentazione di rete — È consigliato l'uso di un interruttore di alimentazione di rete per eseguire il fencing in un cluster di livello enterprise.
- Interruttore del Fibre Channel — Un interruttore del Fibre Channel fornisce un accesso allo storage del Fibre Channel. Altre opzioni sono disponibili in base al tipo di interfaccia, per esempio, iSCSI. Un interruttore di questo tipo può essere configurato per eseguire il processo di fencing.
- Storage — Per il cluster sono necessari alcuni tipi di storage. Il tipo dipende dallo scopo del cluster.

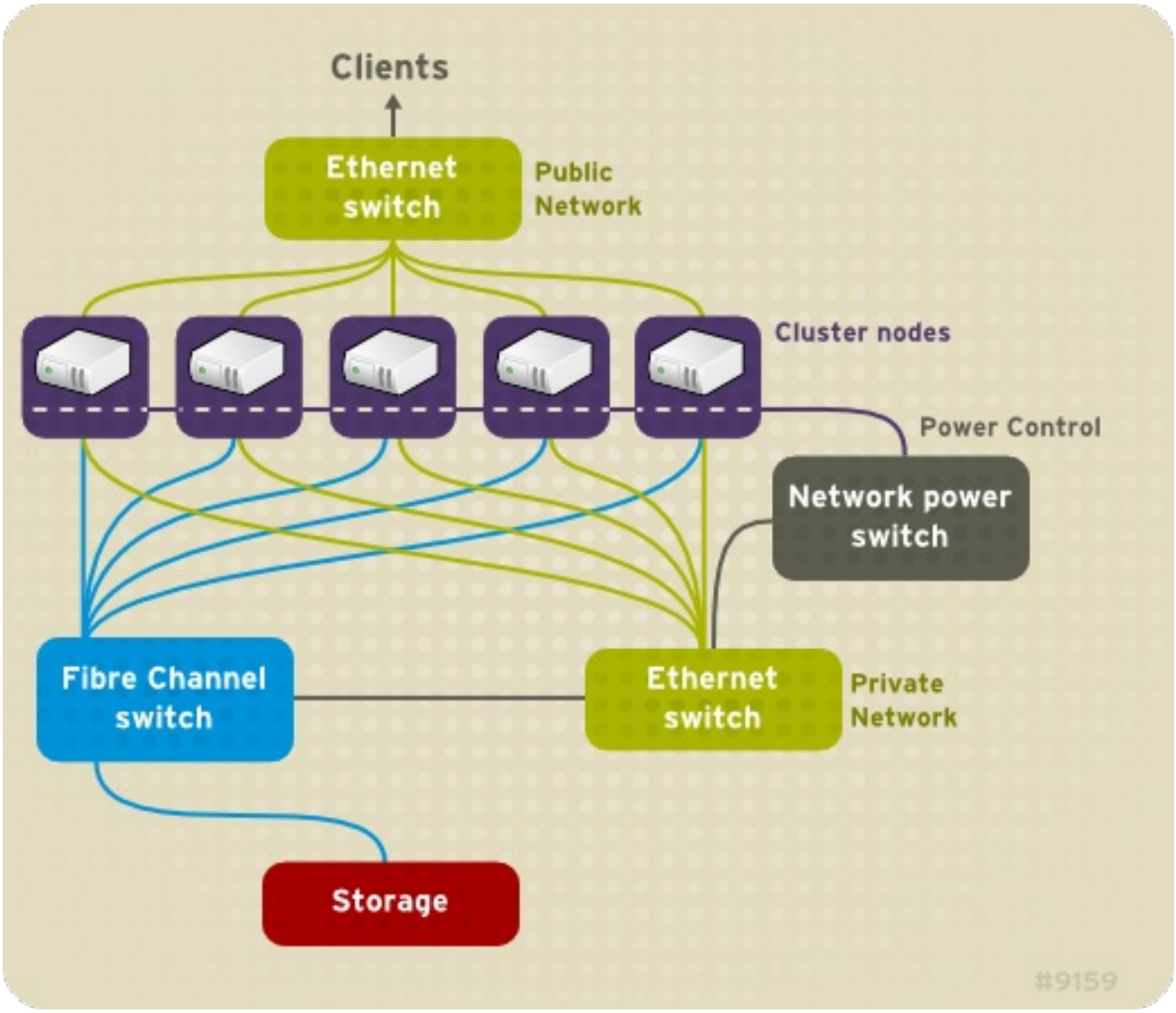


Figura 1.1. Panoramica sull'hardware di Red Hat High Availability Add-On

1.4. INSTALLAZIONE SOFTWARE DI RED HAT HIGH AVAILABILITY ADD-ON

Per installare Red Hat High Availability Add-On software è necessario essere in possesso degli entitlement richiesti per il software. Se utilizzate la GUI di configurazione di **luci**, sarà possibile usare la GUI per l'installazione del software del cluster. Se utilizzate altri strumenti per la configurazione, soddisfate i parametri di sicurezza desiderati ed installate il software in modo simile al software di Red Hat Enterprise Linux.

Usare il seguente comando **`yum install`** per installare i pacchetti del software di Red Hat High Availability Add-On:

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

Da notare che la sola installazione di **`rgmanager`** installerà tutte le dipendenze necessarie per la creazione di un cluster HA dal canale HighAvailability. I pacchetti **`lvm2-cluster`** e **`gfs2-utils`** fanno parte del canale ResilientStorage e potrebbero essere a voi non necessari.

Aggiornamento del software Red Hat High Availability Add-On

È possibile aggiornare il software del cluster di una release maggiore di Red Hat Enterprise Linux senza rimuovere il cluster da un ambiente di produzione. A tale scopo sarà necessario disabilitare il software su ogni singolo host, aggiornando il software e riavviandolo sull'host interessato.

1. Arrestare tutti i servizi del cluster su un nodo. Per istruzioni su come arrestare il software del cluster su un nodo consultare Sezione 8.1.2, «Arresto del software del cluster». È consigliato riposizionare manualmente le macchine virtuali ed i servizi gestiti dal cluster fuori dall'host prima di arrestare **`rgmanager`**.

2. Eseguire il comando **`yum update`** per aggiornare i pacchetti installati.

3. Riavvio del nodo del cluster o riavvio manuale dei servizi del cluster. Per informazioni su come avviare il software del cluster su un nodo consultate Sezione 8.1.1, «Avvio del software del cluster».

1.5. CONFIGURAZIONE DEL SOFTWARE DI RED HAT HIGH AVAILABILITY ADD-ON

La configurazione del software di Red Hat High Availability Add-On consiste nell'uso dei tool di configurazione per specificare il rapporto tra i componenti del cluster. I seguenti tool di configurazione del cluster sono disponibili con Red Hat High Availability Add-On:

- **Conga** — Questa è una interfaccia utente completa per l'installazione, configurazione e gestione di Red Hat High Availability Add-On. Consultare Capitolo 3, *Configurazione di Red Hat High Availability Add-On con **Conga*** e Capitolo 4, *Gestione di Red Hat High Availability Add-On con **Conga*** per informazioni sulla configurazione e gestione di High Availability Add-On con **Conga**.

- Il comando **`ccs`** — Questa è una interfaccia utente completa per l'installazione, configurazione e gestione di Red Hat High Availability Add-On. Consultare Capitolo 5, *Configurazione di Red Hat High Availability Add-On con il comando **ccs*** e Capitolo 6, *Gestione di Red Hat High Availability Add-On con **ccs*** per informazioni sulla configurazione e gestione di High Availability Add-On con **`ccs`**.

- Tool della linea di comando — Questo è un insieme di tool della linea di comando per la configurazione e gestione di Red Hat High Availability Add-On. Consultare Capitolo 7, *Configurazione di Red Hat High Availability Add-On con i tool della linea di comando* e Capitolo 8, *Gestione di Red Hat High Availability Add-On con i tool della linea di comando* per informazioni sulla configurazione e gestione di un cluster usando i tool della linea di comando. Consultare Appendice E, *Sommario dei tool della linea di comando* per un sommario dei tool preferiti.

NOTA

`system-config-cluster` non è disponibile in Red Hat Enterprise Linux 6.

CAPITOLO 2. PRIMA DI CONFIGURARE RED HAT HIGH AVAILABILITY ADD-ON

Questo capitolo descrive le considerazioni ed i compiti da eseguire prima di installare e configurare il Red Hat High Availability Add-On, e consiste nelle seguenti sezioni.

IMPORTANTE

Assicuratevi che l'implementazione di Red Hat High Availability Add-On possa essere supportata ed in grado di soddisfare i vostri requisiti. Consultate un rappresentante autorizzato di Red Hat per una verifica della configurazione prima dell'impiego. In aggiunta assegnate un periodo di prova per le varie modalità d'errore.

2.1. CONSIDERAZIONI GENERALI SULLA CONFIGURAZIONE

È possibile configurare Red Hat High Availability Add-On in modi diversi per soddisfare le vostre esigenze. Considerate quanto di seguito riportato durante le fasi di pianificazione, configurazione ed implementazione.

Numero di nodi supportati del cluster

Il numero massimo di nodi del cluster supportati da High Availability Add-On è 16.

Cluster con sito singolo

Solo i cluster con un solo sito sono completamente supportati. Non sono supportati invece i cluster che si estendono su posizioni fisiche multiple. Per maggiori informazioni sui cluster con siti multipli contattare un rappresentante per il supporto o alle vendite di Red Hat.

GFS2

Anche se il file system GFS2 può essere implementato in un sistema standalone o come parte di una configurazione del cluster, Red Hat non supporta l'uso del GFS2 come file system con nodo singolo. Red Hat supporta un numero di file system di nodi singoli ad elevate prestazioni ottimizzati per i singoli nodi e quindi con un overhead più basso rispetto ad un file system del cluster. Red Hat consiglia l'uso dei suddetti file system rispetto al GFS2 nel caso in cui si verifichi la necessità di un montaggio del file system da parte del nodo. Red Hat continuerà a supportare GFS2 come file system con un solo nodo per i propri utenti.

Quando configurate un file system GFS2 come file system del cluster assicuratevi che tutti i nodi presenti in un cluster abbiano accesso allo storage condiviso. Configurazioni asimmetriche nelle quali solo alcuni nodi hanno un accesso allo storage condiviso, non saranno supportate. Ciò non richiederà il montaggio da parte di tutti i nodi del file system GFS2.

Configurazione hardware No-single-point-of-failure

I cluster possono includere un array dual-controller RAID, canali di rete multipli collegati, percorsi multipli tra i membri del cluster e lo storage, e sistemi un-interruptible power supply (UPS) ridondanti per assicurare che nessun errore singolo possa causare un arresto dell'applicazione o una perdita di dati.

Alternativamente sarà possibile impostare un cluster low-cost in modo da fornire una disponibilità più bassa rispetto ad un cluster no-single-point-of-failure. Per esempio, è possibile impostare un cluster con un RAID array con controllore singolo ed un solo canale Ethernet.

Alcune alternative low-cost, ad esempio i controllori RAID dell'host, di software RAID senza un supporto cluster e configurazioni SCSI parallele multi-initiator non sono compatibili o appropriate per un loro uso come storage del cluster condiviso.

Garantire l'integrità dei dati

Per assicurare l'integrità dei dati solo un nodo per volta può eseguire un servizio o accedere ai dati relativi al servizio del cluster. L'uso degli interruttori di alimentazione in una configurazione hardware del cluster permette ad un nodo di eseguire un ciclo di alimentazione di un altro nodo prima di riavviare i servizi HA del nodo in questione durante un processo di failover. Tale operazione impedisce a due nodi di accedere simultaneamente ai dati corrompendoli. È fortemente consigliato l'uso dei *dispositivi di fencing* (soluzioni hardware o software che eseguono una alimentazione remota, l'arresto ed il riavvio dei nodi del cluster) per garantire una integrità dei dati in tutte le condizioni d'errore.

Aggregazione del canale ethernet

Il quorum del cluster e lo stato del nodo vengono determinati per mezzo di una comunicazione tra i nodi del cluster tramite Ethernet. In aggiunta i nodi del cluster usano Ethernet per una varietà di altre funzioni critiche del cluster (per esempio il fencing). Con Ethernet channel bonding, le interfacce multiple di Ethernet sono configurate in modo da comportarsi come se fossero una, riducendo il rischio di un single-point-of-failure in una connessione tipica di Ethernet tra i nodi del cluster ed altre sezioni hardware.

Con Red Hat Enterprise Linux 6.4 sono supportate le modalità 0, 1, e 2 per il bonding.

IPv4 e IPv6

High Availability Add-On supporta i protocolli internet IPv4 e IPv6. Il supporto per IPv6 con l'High Availability Add-On rappresenta una nuova funzione con Red Hat Enterprise Linux 6.

2.2. HARDWARE COMPATIBILE

Prima di configurare il software di Red Hat High Availability Add-On assicuratevi che il cluster utilizzi l'hardware appropriato (per esempio i dispositivi di fencing appropriati, i dispositivi di storage e gli interruttori Fibre Channel). Consultare le linee guida per la configurazione hardware su http://www.redhat.com/cluster_suite/hardware/ per le informazioni più recenti sulla compatibilità.

2.3. ABILITARE LE PORTE IP

Prima di implementare il Red Hat High Availability Add-On abilitare le porte IP specifiche sui nodi del cluster e sui computer che eseguono **luci** (il server dell'interfaccia utente di **Conga**). Le seguenti sezioni identificano le porte IP da abilitare:

- Sezione 2.3.1, «Come abilitare le porte IP sui nodi del cluster»
- Sezione 2.3.2, «Come abilitare la porta IP per **luci**»

La seguente sezione fornisce le regole **`iptables`** per abilitare le porte IP necessarie a Red Hat High Availability Add-On:

- Sezione 2.3.3, «Configurazione del firewall di iptables per abilitare i componenti del cluster»

2.3.1. Come abilitare le porte IP sui nodi del cluster

Per permettere ai nodi presenti in un cluster di comunicare tra loro è necessario abilitare le porte IP assegnate a determinati componenti di Red Hat High Availability Add-Ons. Tabella 2.1, «Porte IP abilitate sui nodi di Red Hat High Availability Add-On» elenca i numeri delle porte IP, i protocolli relativi ed i componenti ai quali sono assegnati i numeri delle porte. Ad ogni nodo abilitare le porte IP consultando Tabella 2.1, «Porte IP abilitate sui nodi di Red Hat High Availability Add-On». Per abilitare le porte IP usare **`system-config-firewall`**.

Tabella 2.1. Porte IP abilitate sui nodi di Red Hat High Availability Add-On

Numero porta IP	Protocollo	Componente
5404, 5405	UDP	**`corosync/cman`** (Cluster Manager)
11111	TCP	**`ricci`** (inoltra le informazioni aggiornate del cluster)
21064	TCP	**`dlm`** (Distributed Lock Manager)
16851	TCP	**`modclusterd`**

2.3.2. Come abilitare la porta IP per luci

Per permettere ai client di comunicare con un computer che esegue **luci** (il server dell'interfaccia utente di **Conga**), sarà necessario abilitare la porta IP assegnata a **luci**. Per ogni computer che esegue **luci** abilitare la porta IP consultando Tabella 2.2, «Porta IP abilitata su un computer che esegue **luci**».

NOTA

La porta 11111 dovrebbe essere già abilitata se il nodo di un cluster esegue **luci**.

Tabella 2.2. Porta IP abilitata su un computer che esegue luci

Numero porta IP	Protocollo	Componente
8084	TCP	**luci** (server interfaccia utente di **Conga**)

Con Red Hat Enterprise Linux 6.1, il quale permette di abilitare la configurazione per mezzo di **/etc/sysconfig/luci**, è possibile configurare l'unico indirizzo IP al quale viene servito **luci**. È possibile utilizzare questa funzione se l'infrastruttura del server presenta più di una rete e desiderate accedere **luci** solo da una rete interna. Per fare questo decommentare e modificare la riga presente nel file corrispondente all'**host**. Per esempio, per modificare l'impostazione **host** nel file su 10.10.10.10, modificare la riga **host** nel modo seguente:

```
host = 10.10.10.10
```

Per maggiori informazioni sul file **/etc/sysconfig/luci**, consultare Sezione 2.4, «Configurazione di **luci** con **/etc/sysconfig/luci**».

2.3.3. Configurazione del firewall di iptables per abilitare i componenti del cluster

Di seguito vengono riportati alcuni esempi di regole iptable per abilitare le porte IP necessarie a Red Hat Enterprise Linux 6 (with High Availability Add-on). Da notare che questi esempi usano 192.168.1.0/24 come subnet, a tale scopo sostituire 192.168.1.0/24 con la subnet appropriata se usate queste regole.

Per **cman** (Cluster Manager), usare i seguenti filtri.

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

Per **dlm** (Distributed Lock Manager):

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

Per **ricci** (parte del Conga remote agent):

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

Per **modclusterd** (parte del Conga remote agent):

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

Per **luci** (Conga User Interface server):

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

Per **igmp** (Internet Group Management Protocol):

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

Dopo l'esecuzione dei suddetti comandi eseguite quanto di seguito riportato per salvare la configurazione corrente e renderla persistente durante il riavvio.

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

2.4. CONFIGURAZIONE DI LUCI CON /ETC/SYSCONFIG/LUCI

Con Red Hat Enterprise Linux 6.1 è possibile configurare alcuni aspetti del comportamento di **luci** per mezzo del file **/etc/sysconfig/luci**. I parametri modificabili includono le impostazioni ausiliari dell'ambiente in esecuzione usate da init script e da una configurazione del server. Sarà possibile altresì modificare questo file per cambiare alcuni parametri di configurazione dell'applicazione . All'interno del file sono presenti alcune istruzioni che descrivono quali sono i parametri modificabili tramite questo file.

Durante la modifica del file per proteggere il formato desiderato non modificate le righe che non sono corrispondenti alla configurazione del file **/etc/sysconfig/luci**. È importante altresì seguire la sintassi di questo file ed in particolare per la sezione **INITSCRIPT**, la quale non permette di avere la presenza di spazi intorno al carattere uguale e richiede l'uso di virgolette per racchiudere le righe che presentano spazi.

Il seguente esempio mostra come modificare la porta attraverso la quale viene servito **luci** tramite la modifica del file **/etc/sysconfig/luci**.

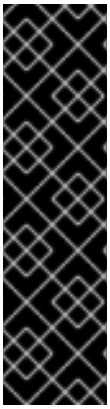
1. Decommentare la seguente riga nel file **/etc/sysconfig/luci**:

   ```
   #port = 4443
   ```

2. Sostituire 4443 con il numero di porta desiderato con un valore uguale o superiore a 1024 (non una porta privilegiata). Per esempio, modificare la riga del file nel modo seguente per impostare la porta su 8084 per mezzo della quale viene servito **luci**.

   ```
   port = 8084
   ```

3. Riavviare il servizio **luci** per implementare le modifiche.



IMPORTANTE

Quando modificate il parametro di configurazione nel file **/etc/sysconfig/luci** per ridefinire un valore predefinito, fate attenzione ad usare il valore appena impostato. Per esempio, quando modificate la porta per mezzo della quale viene servito **luci**, assicuratevi di utilizzare il nuovo valore quando abilitate la porta IP come descritto in Sezione 2.3.2, «Come abilitare la porta IP per **luci**».

I parametri host e quelli modificati verranno riportati automaticamente nell'URL visualizzato all'avvio del servizio **luci** come descritto in Sezione 3.2, «Avvio di **luci**». Per accedere **luci** utilizzare questo URL.

Per informazioni complete sui parametri modificabili con il file **/etc/sysconfig/luci** consultate la documentazione presente all'interno del file in questione.

2.5. CONFIGURAZIONE DI ACPI PER L'USO CON DISPOSITIVI DI FENCING INTEGRATI

Se il cluster utilizza i dispositivi di fencing integrati sarà necessario configurare ACPI (Advanced Configuration and Power Interface) per assicurare un fencing immediato e completo.

NOTA

Per le informazioni più aggiornate sui dispositivi di fencing integrati supportati da Red Hat High Availability Add-On, consultate http://www.redhat.com/cluster_suite/hardware/.

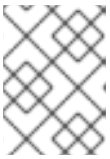
Se un nodo del cluster è configurato per essere isolato da un dispositivo di fencing integrato disabilitate ACPI Soft-Off per il nodo in questione. Disabilitando ACPI Soft-Off permetterete ad un dispositivo di fencing integrato di disabilitare completamente ed immediatamente un nodo invece di eseguire un arresto normale 'clean shutdown' (per esempio **`shutdown -h now`**). In caso contrario se ACPI Soft-Off è abilitato, un dispositivo di fencing integrato avrà bisogno di quattro o più secondi per disabilitare il nodo (consultare la nota seguente). In aggiunta se ACPI Soft-Off è abilitato e si verifica una sospensione o un panic del nodo durante l'arresto, il dispositivo di fencing integrato potrebbe non essere in grado di disabilitare il nodo. In queste condizioni l'isolamento del nodo potrebbe essere ritardato o potrebbe non avere successo. Di conseguenza quando un nodo è isolato con un dispositivo di fencing integrato e ACPI Soft-Off è abilitato, il processo di ripristino del cluster è più lento oppure sarà necessario un intervento amministrativo.

NOTA

La quantità di tempo necessaria per isolare un nodo dipende dal dispositivo di fencing integrato. Alcuni dispositivi eseguono l'operazione equivalente a quella di premere e mantenere premuto il tasto di alimentazione; Per questo motivo il dispositivo di fencing disabilita il nodo in quattro o cinque secondi. Altri dispositivi eseguono una operazione equivalente a quella del tasto di alimentazione, affidandosi al sistema operativo per disabilitare il nodo; quindi il dispositivo di fencing disabilita il nodo in un periodo di tempo maggiore ai quattro o cinque secondi.

Per disabilitare ACPI Soft-Off usare **`chkconfig`** e verificare che il nodo sia stato disabilitato immediatamente dopo l'isolamento. Il metodo preferito per disabilitare ACPI Soft-Off è con **`chkconfig`**: tuttavia se il metodo non risulta essere il più idoneo per il cluster potrete disabilitare ACPI Soft-Off con uno dei seguenti metodi:

- Modifica delle impostazione del BIOS su "instant-off" o una impostazione equivalente che disabilita il nodo senza alcun ritardo

  NOTA

  In alcuni computer potrebbe non essere possibile disabilitare ACPI Soft-Off con il BIOS

- Aggiungere **`acpi=off`** alla linea di comando d'avvio del kernel del file **`/boot/grub/grub.conf`**

IMPORTANTE

Questo metodo disabilita completamente ACPI; alcuni computer non eseguono un avvio corretto se ACPI è completamente disabilitato. Usare questo metodo *solo* se altri metodi non sono idonei al cluster.

Le seguenti sezioni contengono le procedure per il metodo preferito insieme ai metodi alternativi sulla disabilitazione di ACPI Soft-Off:

- Sezione 2.5.1, «Disabilitare ACPI Soft-Off con **chkconfig**» — Metodo preferito
- Sezione 2.5.2, «Disabilitare ACPI Soft-Off con il BIOS» — Primo metodo alternativo
- Sezione 2.5.3, «Disabilitare completamente ACPI nel file **grub.conf**» — Secondo metodo alternativo

2.5.1. Disabilitare ACPI Soft-Off con `chkconfig`

È possibile usare **chkconfig** per disabilitare ACPI Soft-Off rimuovendo il demone ACPI (**acpid**) da **chkconfig** o disabilitando **acpid**.

NOTA

Questo è il metodo preferito per disabilitare ACPI Soft-Off.

Disabilitare ACPI Soft-Off con **chkconfig** su ogni nodo del cluster nel modo seguente:

1. Eseguire uno dei seguenti comandi:
   - **chkconfig --del acpid** — Questo comando rimuove **acpid** dalla gestione **chkconfig**.

     — O —
   - **chkconfig --level 2345 acpid off** — Questo comando disabilita **acpid**.
2. Riavviare il nodo.
3. Dopo aver configurato il cluster, e durante la sua esecuzione, verificare che il nodo sia disabilitato subito dopo essere stato isolato.

NOTA

È possibile isolare il nodo con il comando **fence_node** o **Conga**.

2.5.2. Disabilitare ACPI Soft-Off con il BIOS

Il metodo preferito per disabilitare ACPI Soft-Off è tramite l'uso di **chkconfig** (Sezione 2.5.1, «Disabilitare ACPI Soft-Off con **chkconfig**»). Tuttavia se il metodo preferito non è efficace seguire la procedura di seguito indicata.

NOTA

In alcuni computer potrebbe non essere possibile disabilitare ACPI Soft-Off con il BIOS

È possibile disabilitare ACPI Soft-Off attraverso la configurazione del BIOS di ogni nodo del cluster nel modo seguente:

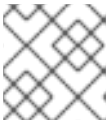
1. Riavviare il nodo ed iniziare il programma **`BIOS CMOS Setup Utility`**.
2. Andate sul menu **Alimentazione** (o menu equivalente per la gestione dell'alimentazione).
3. Sul menu **Alimentazione** impostare la funzione **Soft-Off con PWR-BTTN** (o equivalente) su **Instant-Off** (o impostazione equivalente che disabilita il nodo tramite il pulsante di alimentazione senza ritardi). Esempio 2.1, «**`BIOS CMOS Setup Utility`**: **Soft-Off by PWR-BTTN** impostato su **Instant-Off**» mostra un menu **Alimentazione** con **Funzione ACPI** impostata su **Abilita** e **Soft-Off con PWR-BTTN** impostata su **Instant-Off**.

   NOTA

   Le funzioni equivalenti di **Funzione ACPI**, **Soft-Off con PWR-BTTN**, e **Instant-Off** possono variare in base ai computer. Tuttavia lo scopo di questa procedura è quello di configurare il BIOS in modo tale che il computer venga disabilitato tramite il pulsante di alimentazione senza alcun ritardo.

4. Uscire dal programma **`BIOS CMOS Setup Utility`** salvando la configurazione del BIOS.
5. Dopo aver configurato il cluster, e durante la sua esecuzione, verificare che il nodo sia disabilitato subito dopo essere stato isolato.

   NOTA

   È possibile isolare il nodo con il comando **`fence_node`** o **Conga**.

Esempio 2.1. `BIOS CMOS Setup Utility`: Soft-Off by PWR-BTTN impostato su Instant-Off

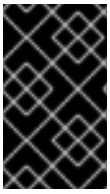
```
+---------------------------------------------|-------------------+
|    ACPI Function             [Enabled]      |    Item Help      |
|    ACPI Suspend Type         [S1(POS)]      |-------------------|
|  x Run VGABIOS if S3 Resume   Auto          |   Menu Level   *  |
|    Suspend Mode              [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       |                   |
```

```
|                                                |                   |
|                                                |                   |
+------------------------------------------------|-------------------+
```

Questo esempio mostra la **Funzione ACPI** impostata su **Enabled**, e **Soft-Off by PWR-BTTN** impostata su **Instant-Off**.

2.5.3. Disabilitare completamente ACPI nel file `grub.conf`

Il metodo preferito per disaiblitare ACPI Soft-Off è utilizzando **`chkconfig`** (Sezione 2.5.1, «Disabilitare ACPI Soft-Off con **`chkconfig`**»). Tuttavia se il metodo preferito non è efficace sarà possibile disabilitare ACPI Soft-Off tramite la gestione dell'alimentazione del BIOS (Sezione 2.5.2, «Disabilitare ACPI Soft-Off con il BIOS»). Se entrambi i metodi non sono idonei disabilitare completamente ACPI aggiungendo **`acpi=off`** sulla linea di comando d'avvio nel file **`grub.conf`**.



IMPORTANTE

Questo metodo disabilita completamente ACPI; alcuni computer non eseguono un avvio corretto se ACPI è completamente disabilitato. Usare questo metodo *solo* se altri metodi non sono idonei al cluster.

È possibile disabilitare completamente ACPI modificando il file **`grub.conf`** di ogni nodo nel modo seguente:

1. Aprire **`/boot/grub/grub.conf`** con un editor di testo.
2. Aggiungere **`acpi=off`** sulla linea di comando d'avvio del kernel in **`/boot/grub/grub.conf`** (consultare Esempio 2.2, «Linea di comando d'avvio del kernel con **`acpi=off`**»).
3. Riavviare il nodo.
4. Dopo aver configurato il cluster, e durante la sua esecuzione, verificare che il nodo sia disabilitato subito dopo essere stato isolato.

NOTA

È possibile isolare il nodo con il comando **`fence_node`** o **Conga**.

Esempio 2.2. Linea di comando d'avvio del kernel con `acpi=off`

```
# 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
```

In questo esempio **acpi=off** è stato aggiunto alla linea di comando d'avvio del kernel — la riga che inizia con "kernel /vmlinuz-2.6.32-193.el6.x86_64.img".

2.6. CONSIDERAZIONI PER LA CONFIGURAZIONE DEI SERVIZI HA

Sarà possibile creare un cluster per soddisfare i requisiti di elevata disponibilità configurando servizi HA (high-availability). Il componente chiave per la gestione del servizio HA con Red Hat High Availability Add-On, **rgmanager**, implementa un cold failover per applicazioni commerciali. Con Red Hat High Availability Add-On un'applicazione è configurata con altre risorse del cluster in modo da formare un servizio HA in grado di eseguire il failover da un nodo ad un altro del cluster, senza alcuna interruzione apparente per i client. Un failover del servizio HA si verifica quando un nodo del cluster fallisce o se un amministratore del sistema cluster sposta il servizio da un nodo ad un altro (per esempio per una interruzione del servizio pianificata di un nodo del cluster)

Per creare un servizio HA sarà necessario configurarlo nel file di configurazione del cluster. Un servizio HA comprende le *risorse* del cluster. Le risorse sono blocchi creati e gestiti nel file di configurazione del cluster — per esempio un indirizzo IP, uno script di inizializzazione dell'applicazione o una partizione condivisa GFS2 di Red Hat.

Un servizio HA può essere eseguito su un solo nodo per volta per conservare l'integrità dei dati. È possibile specificare una priorità di failover in un dominio di failover. Specificando la priorità si assegnerà un livello di priorità ad ogni nodo in un dominio di failover. Il livello di priorità determina l'ordine di failover — e determinana così quale nodo sarà usato dal servizio in presenza di un failover. Se non specificate alcuna priorità, il failover di un servizio HA potrà verificarsi su qualsiasi nodo nel proprio dominio di failover. Altresì sarà possibile specificare se un servizio HA è limitato ad una esecuzione su nodi del proprio dominio di failover associato. (Quando associato con un dominio non limitato un servizio HA è in grado di avviarsi su qualsiasi nodo se nessun membro del dominio di failover è disponibile.)

Figura 2.1, «Esempio servizio del cluster del Web Server» mostra un esempio di servizio HA sotto forma di web server chiamato "content-webserver". Eseguito in un nodo B del cluster ed è in un dominio di failover il quale consiste nei nodi A, B e C. In aggiunta, il dominio di failover è configurato con una priorità di failover in modo da usare il nodo D prima del nodo A e limitare il failover solo sui nodi presenti in quel dominio. Il servizio HA comprende le seguenti risorse del cluster:

- Risorsa indirizzo IP — Indirizzo IP 10.10.10.201.
- Una risorsa dell'applicazione chiamata "httpd-content" — un init script dell'applicazione del web server **/etc/init.d/httpd** (il quale specifica **httpd**).
- Una risorsa del file system — Red Hat GFS2 chiamata "gfs2-content-webserver".

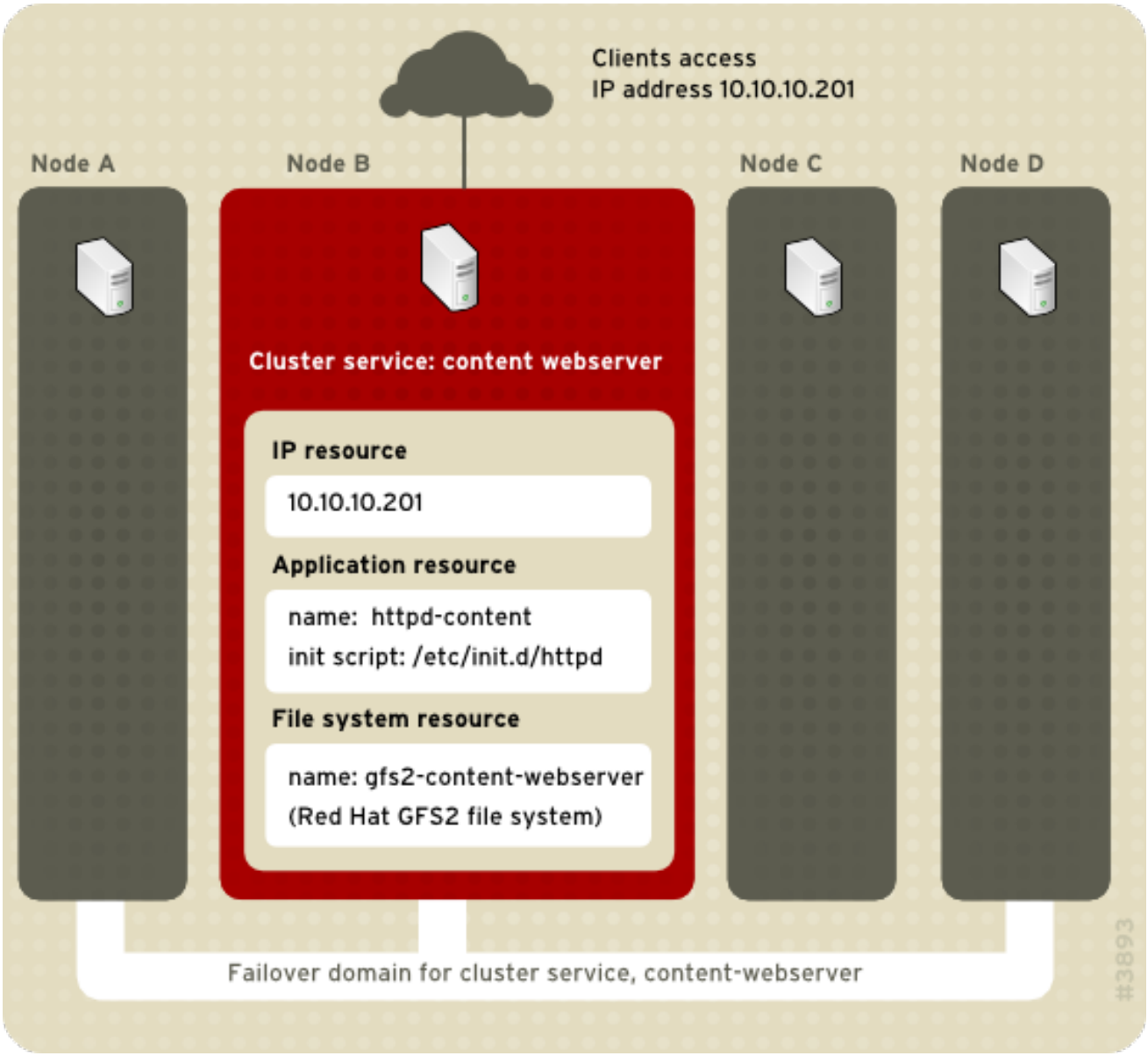


Figura 2.1. Esempio servizio del cluster del Web Server

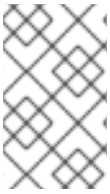
I client accedono al servizio HA attraverso l'indirizzo IP 10.10.10.201, permettendo così una interazione con l'applicazione del web server httpd-content. L'applicazione httpd-content utilizza il file system gfs2-content-webserver. Se il nodo B fallisce, il servizio HA content-webserver verrà passato sul nodo D. Se il nodo D a sua volta non è disponibile il servizio sarà passato sul nodo A. Il failover verrà eseguito con un livello di interruzione minimo nei confronti dei client del cluster. Per esempio, in un servizio HTTP, è possibile perdere informazioni specifiche relative allo stato (come ad esempio i dati della sessione). Il servizio HA sarà accessibile da un nodo diverso usando lo stesso indirizzo IP usato prima del failover.

NOTA

Per maggiori informazioni sui servizi HA e domini di failover consultare la *Panoramica High Availability Add-On*. Per maggiori informazioni sulla configurazione dei domini di failover consultare Capitolo 3, *Configurazione di Red Hat High Availability Add-On con **Conga***(usando **Conga**) o Capitolo 7, *Configurazione di Red Hat High Availability Add-On con i tool della linea di comando* (usando le utilità della linea di comando).

Un servizio HA rappresenta un gruppo di risorse del cluster configurato in una entità omogenea in grado di fornire servizi specializzati ai client. Un servizio HA è rappresentato da un albero delle risorse nel file di configurazione del cluster, **`/etc/cluster/cluster.conf`** (in ogni nodo del cluster). Nel file di

configurazione del cluster, ogni albero è una rappresentazione XML la quale specifica ogni risorsa, gli attributi e l'appartenenza tra le altre risorse presenti nell'albero delle risorse (genitore, figlio o altro tipo di parentela).



NOTA

Poichè un servizio HA consiste in risorse organizzate in un albero gerarchico, un servizio viene generalmente indicato come un *albero delle risorse* o *gruppo di risorse*. Entrambi sono sinonimi di *servizio HA*.

Alla radice di ogni albero delle risorse è presente una risorsa speciale — *risorsa del servizio*. Altri tipi di risorse formano il resto del servizio determinando così le proprie caratteristiche. La configurazione di un servizio HA consiste nella creazione di una risorsa del servizio, creazione di risorse del cluster subordinate, ed organizzazione delle stesse in una entità omogenea conforme alle restrizioni gerarchiche del servizio.

Prima di configurare un servizio HA considerare due requisiti importanti:

- Il tipo di risorse necessarie per creare un servizio
- Rapporti di parentela, genitore, e figlio tra le risorse

Il tipo di risorse e la gerarchia dipendono dal tipo di servizio che state configurando.

I tipi di risorse del cluster sono elencati in Appendice B, *Parametri della risorsa HA*. Le informazioni sui rapporti di parentela, figlio e genitore sono riportate in Appendice C, *Comportamento delle risorse HA*.

2.7. CONVALIDA DELLA CONFIGURAZIONE

La configurazione del cluster viene convalidata automaticamente in base allo schema del cluster su **`/usr/share/cluster/cluster.rng`** durante l'avvio ed il ricaricamento di una configurazione. È possibile convalidare una configurazione in qualsiasi momento usando il comando **`ccs_config_validate`**. Per informazioni sulla convalida della configurazione durante l'uso del comando **`ccs`** consultare Sezione 5.1.6, «Convalida della configurazione».

È disponibile uno schema per una revisione su **`/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html`** (per esempio **`/usr/share/doc/cman-3.0.12/cluster_conf.html`**).

La convalida della configurazione controlla la presenza dei seguenti errori:

- Validità XML — Controlla che il file di configurazione sia un file XML valido.
- Opzioni della configurazione — Controlla che le opzioni siano valide (elementi ed attributi XML).
- Valori delle opzioni — Controlla che le opzioni contengano i dati validi (limitati).

I seguenti esempi mostrano configurazioni valide e non valide e riportano i controlli di validità:

- Configurazione valida — Esempio 2.3, «**`cluster.conf`** Configurazione d'esempio: File valido»
- XML non valido — Esempio 2.4, «**`cluster.conf`** Configurazione d'esempio: XML non valido»
- Opzione non valida — Esempio 2.5, «**`cluster.conf`** Configurazione d'esempio: Opzione non valida»

- Valore opzione non valido — Esempio 2.6, «**cluster.conf** Configurazione d'esempio: Valore opzione non valido»

Esempio 2.3. cluster.conf Configurazione d'esempio: File valido

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

Esempio 2.4. cluster.conf Configurazione d'esempio: XML non valido

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

In questo esempio nell'ultima riga della configurazione (indicata come "INVALID") manca uno slash — La riga risulta essere **<cluster>** invece di **</cluster>**.

Esempio 2.5. `cluster.conf` Configurazione d'esempio: Opzione non valida

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

In questo esempio la seconda riga della configurazione (indicata come "INVALID") contiene un elemento XML non valido — La riga risulta essere **loging** invece di **logging**.

Esempio 2.6. `cluster.conf` Configurazione d'esempio: Valore opzione non valido

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

```
          <fence>
          </fence>
        </clusternode>
      </clusternodes>
      <fencedevices>
      </fencedevices>
      <rm>
      </rm>
  <cluster>
```

In questo esempio la quarta riga della configurazione (indicata come "INVALID") contiene un valore non valido per l'attributo XML, **nodeid** nella riga **clusternode** per **node-01.example.com**. Ne risulta un valore negativo ("-1") invece di un valore positivo ("1"). Per l'attributo **nodeid** il valore deve essere positivo.

2.8. CONSIDERAZIONI PER IL NETWORKMANAGER

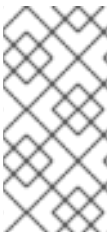
L'uso di **NetworkManager** non è supportato sui nodi del cluster. Se avete installato **NetworkManager** sui nodi, rimuovetelo o disabilitatelo.

NOTA

Il servizio **cman** non verrà avviato se **NetworkManager** è in esecuzione o se è stato configurato per una esecuzione con il comando **chkconfig**.

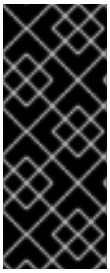
2.9. CONSIDERAZIONI SULL'USO DEL QUORUM DISK

Quorum Disk è un demone del quorum basato sul disco, **qdiskd**, in grado di fornire parametri euristici supplementari per determinare l'idoneità dei nodi. Con i suddetti valori sarà possibile determinare i fattori importanti per il funzionamento corretto del nodo in presenza di una partizione della rete. Per esempio, in un cluster a quattro nodi con una divisione di 3:1, generalmente i tre nodi automaticamente "vincono" a causa del rapporto di maggioranza di tre a uno. In queste circostanze il nodo rimasto solo viene isolato. Tuttavia con **qdiskd** sarà possibile impostare i parametri euristici in modo da permettere al nodo di vincere in base all'accesso ad una risorsa critica (per esempio un percorso di rete critico). Se il vostro cluster necessita di metodi aggiuntivi per determinare lo stato di un nodo allora configurate **qdiskd** in modo da soddisfarne i requisiti.



NOTA

Se non sono presenti requisiti speciali per la salute del nodo non sarà necessario configurare **qdiskd**. Un esempio di requisito speciale è una configurazione "all-but-one". In questa configurazione **qdiskd** viene configurato in modo da fornire un numero di voti sufficienti da mantenere il quorum anche se solo un nodo risulta in funzione.



IMPORTANTE

In generale i parametri euristici ed altri parametri **qdiskd** per la vostra implementazione dipendono dalll'ambiente del sito e dai requisiti speciali. Per comprendere l'uso dei parametri euristici e di altri parametri **qdiskd** consultate la pagina man qdisk(5). Se avete bisogno di qualsiasi assistenza per la comprensione e l'uso di **qdiskd** contattate un rappresentante autorizzato di Red Hat.

Se avete bisogno di utilizzare **qdiskd** considerate quanto di seguito riportato:

Voti del nodo del cluster

Quando si utilizza un Quorum Disk ogni nodo del cluster deve avere un voto.

Valore di timeout di appartenenza CMAN

Il valore di timeout di appartenenza CMAN (il tempo entro il quale se un nodo non risulta attivo CMAN lo ritiene terminato e quindi non membro) dovrà essere almeno il doppio del valore di timeout di appartenzenza di **qdiskd**. Così facendo il demone del quorum avrà tempo sufficiente per rilevare i nodi falliti e potrà eseguire tale operazione con un tempo superiore rispetto a CMAN. Il valore predefinito per il timeout di appartenenza CMAN è 10 secondi. Altre condizioni specifiche al sito potrebbero interessare l'appartenenza tra i valori di timeout di CMAN e **qdiskd**. Per l'assistenza sulla regolazione del valore di timeout di appartenenza CMAN contattate un rappresentante autorizzato di Red Hat.

Fencing

Per un isolamento corretto durante l'utilizzo di **qdiskd** usare il power fencing. Anche se altri tipi di fencing possono essere idonei per cluster non configurati con **qdiskd**, essi potrebbero essere non idonei per cluster configurati con **qdiskd**.

Numero massimo di nodi

Un cluster configurato con **qdiskd** supporta un massimo di 16 nodi. Questo limite è stato impostato per motivi di scalabilità; aumentando il numero di nodi aumenterà l'I/O sincrono sul dispositivo quorum disk condiviso.

Dispositivo quorum disk

Un dispositivo quorum disk dovrebbe essere un dispositivo a blocchi condiviso con un accesso simultaneo lettura/scrittura da parte di tutti i nodi in un cluster. La dimensione minima del dispositivo a blocchi è di 10 Megabyte. Esempi di dispoisitivi a blocchi condivisi utilizzabili da **qdiskd** sono i multi-port SCSI RAID array, un Fibre Channel RAID SAN, o un target iSCSI configurato-RAID. È possibile creare un dispositivo quorum disk con **mkqdisk**, l'utilità quorum disk del cluster. Per informazioni sull'utilizzo dell'utilità consultate la pagina man di mkqdisk(8).

NOTA

Non è consigliato l'uso di JBOD come quorum disk. JBOD non è in grado di fornire prestazioni affidabili e non permette quindi ad un nodo di eseguire un processo di scrittura con una velocità sufficiente. Se un nodo non è in grado di eseguire una scrittura sul dispositivo del quorum disk con la velocità richiesta, il nodo verrà rimosso dal cluster.

2.10. RED HAT HIGH AVAILABILITY ADD-ON E SELINUX

High Availability Add-On per Red Hat Enterprise Linux 6 supporta SELinux con uno stato **enforcing** e SELinux impostato su **targeted**.

Per maggiori informazioni su SELinux consultate la *Deployment Guide* per Red Hat Enterprise Linux 6.

2.11. INDIRIZZI MULTICAST

I nodi presenti in un cluster comunicano tra loro usando indirizzi multicast. Per questo motivo ogni interruttore di rete ed elementi per il networking associati in Red Hat High Availability Add-On, devono essere configurati per poter abilitare gli indirizzi multicast ed avere un supporto IGMP (Internet Group Management Protocol). Assicuratevi che ogni interruttore di rete ed elementi di networking associati in Red Hat High Availability Add-On siano in grado di supportare gli indirizzi multicast e IGMP; a tale scopo assicuratevi che sia IGMP che gli indirizzi multicast siano stati abilitati poichè senza di essi non tutti i nodi potranno partecipare alle attività del cluster, causandone così il suo fallimento; usare UDP unicast in questi ambienti come riportato in Sezione 2.12, «Traffico UDP Unicast».

NOTA

I processi di configurazione degli interruttori di rete e dei dispositivi di networking associati variano in base al prodotto. Consultare la documentazione appropriata del rivenditore o altre informazioni per la configurazione degli interruttori di rete e dei dispositivi di networking associati in modo da abilitare gli indirizzi multicast e IGMP.

2.12. TRAFFICO UDP UNICAST

Con Red Hat Enterprise Linux 6.2 i nodi di un cluster possono comunicare tra loro usando un meccanismo di trasporto UDP Unicast. Tuttavia è consigliato l'uso di un P multicasting per la rete del cluster. UDP Unicast rappresenta una alternativa da usare quando l'IP multicasting non è disponibile.

È possibile configurare Red Hat High-Availability Add-On in modo da usare UDP unicast impostando il parametro **cman transport="udpu"** nel file di configurazione **cluster.conf**. È possibile anche specificare Unicast dalla pagina **Configurazione di rete** dell'interfaccia utente di **Conga** come descritto Sezione 3.5.3, «Configurazioni di rete».

2.13. CONSIDERAZIONI SU RICCI

Con Red Hat Enterprise Linux 6, **ricci** sostituisce **ccsd**. Per questo motivo sarà necessario eseguire **ricci** su ogni nodo del cluster per la diffusione delle informazioni aggiornate sulla configurazione del cluster tramite **cman_tool version -r**, il comando **ccs**, o il server dell'interfaccia utente di **luci**. Avviare **ricci** utilizzando **service ricci start** o abilitandolo al momento del boot tramite **chkconfig**. Per informazioni su come abilitare le porte IP per **ricci**, consultare Sezione 2.3.1, «Come abilitare le porte IP sui nodi del cluster».

Con Red Hat Enterprise Linux 6.1 e versioni più recenti l'uso di **ricci** richiederà l'utilizzo di una password se inoltrate per la prima volta la configurazione del cluster aggiornata da un qualsiasi nodo. La password **ricci** è impostata come utente root dopo l'installazione di **ricci** con il comando **passwd ricci** per l'utente **ricci**.

2.14. CONFIGURAZIONE DI MACCHINE VIRTUALI IN UN AMBIENTE CLUSTERIZZATO

Quando configurate il cluster con le risorse della macchina virtuale utilizzare gli strumenti di **rgmanager** per avviare ed arrestare le macchine virtuali. L'uso di **virsh** per avviare una macchina potrebbe causare l'esecuzione della macchina virtuale in più posizioni corrompendone così i dati.

Per ridurre la possibilità che un amministratore esegua un "doppio-avvio" accidentale delle macchine virtuali usando strumenti cluster e non-cluster in un ambiente clusterizzato, configurare il sistema in modo da poter archiviare i file di configurazione della macchina virtuale in una posizione non-predefinita. L'archiviazione dei file di configurazione in una posizione diversa da quella predefinita, rende più difficoltoso l'avvio di una macchina virtuale usando il comando **virsh**, poichè il file di configurazione risulta essere sconosciuto al comando stesso.

La posizione non-predefinita dei file di configurazione della macchina virtuale può essere in qualsiasi luogo. Il vantaggio di utilizzare una condivisione NFS o un file system GFS2 condiviso è che l'amministratore non ha bisogno di mantenere i file di configurazione sincronizzati sui membri del cluster. Tuttavia è possibile usare una directory locale se l'amministratore mantiene i contenuti dell'intero cluster sincronizzati.

In una configurazione del cluster le macchine virtuali possono fare riferimento alla posizione non-predefinita tramite l'attributo **path** di una risorsa. Da notare che **path** è una directory o set di directory separate da due punti ':' e non un percorso per un file specifico.

AVVERTIMENTO

Il servizio **libvirt-guests** deve essere disabilitato su tutti i nodi che eseguono **rgmanager**. Se una macchina virtuale esegue un avvio automatico o riprende le sue funzioni, ciò potrebbe causare una sua esecuzione in posizioni multiple corrompendo così i dati presenti al suo interno.

Per informazioni sugli attributi delle risorse di una macchina virtuale consultare Tabella B.24, «Virtual Machine».

CAPITOLO 3. CONFIGURAZIONE DI RED HAT HIGH AVAILABILITY ADD-ON CON CONGA

Questo capitolo descrive la configurazione del software di Red Hat High Availability Add-On tramite **Conga**. Per informazioni sull'uso di **Conga** per la gestione di un cluster in esecuzione consultare Capitolo 4, *Gestione di Red Hat High Availability Add-On con **Conga***.

NOTA

Conga è una interfaccia utente grafica usata per gestire Red Hat High Availability Add-On. Tuttavia per usare l'interfaccia in modo corretto è necessario conoscere i concetti di base. Non è consigliato utilizzare le funzioni disponibili per capire i concetti relativi alla configurazione del cluster poichè così facendo il sistema potrebbe non essere in grado di mantenere tutti i servizi in esecuzione in presenza di errori.

Questo capitolo consiste nelle seguenti sezioni:

- Sezione 3.1, «Fasi necessarie per la configurazione»
- Sezione 3.2, «Avvio di **luci**»
- Sezione 3.3, «Controllo accesso di luci»
- Sezione 3.4, «Creazione di un cluster»
- Sezione 3.5, «Proprietà globali del cluster»
- Sezione 3.6, «Configurazione del dispositivo di fencing»
- Sezione 3.7, «Configurazione del processo di fencing per i membri del cluster»
- Sezione 3.8, «Configurazione di un dominio di failover»
- Sezione 3.9, «Configurazione delle risorse globali del cluster»
- Sezione 3.10, «Come aggiungere un servizio ad un cluster»

3.1. FASI NECESSARIE PER LA CONFIGURAZIONE

Di seguito vengono riportate le fasi necessarie per la configurazione del software Red Hat High Availability Add-On con **Conga**.

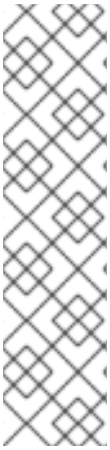
1. Configurazione ed esecuzione dell'interfaccia utente per la configurazione di **Conga** — il server **luci**. Consultare la Sezione 3.2, «Avvio di **luci**».
2. Creazione di un cluster. Consultare Sezione 3.4, «Creazione di un cluster».
3. Configurazione proprietà globali del cluster. Consultare Sezione 3.5, «Proprietà globali del cluster».
4. Configurazione dispositivi di fencing. Consultare la Sezione 3.6, «Configurazione del dispositivo di fencing».
5. Configurazione del fencing per i membri del cluster. Consultare Sezione 3.7, «Configurazione del processo di fencing per i membri del cluster».

6. Creazione dei domini di failover. Consultare Sezione 3.8, «Configurazione di un dominio di failover».

7. Creazione delle risorse. Consultare Sezione 3.9, «Configurazione delle risorse globali del cluster».

8. Creazione dei servizi del cluster. Consultare Sezione 3.10, «Come aggiungere un servizio ad un cluster».

3.2. AVVIO DI LUCI



NOTA

Per utilizzare **luci** nella configurazione di un cluster sarà necessario installare ed eseguire **ricci** sui nodi del cluster come descritto in Sezione 2.13, «Considerazioni su **ricci**». Come riportato in sezione per poter utilizzare **ricci** sarà necessario usare una password richiesta da **luci** per ogni nodo durante la creazione del cluster, come descritto in Sezione 3.4, «Creazione di un cluster».

Prima di avviare **luci** assicuratevi che le porte IP sui nodi del cluster permettano il collegamento alla porta 11111 dal server **luci** su qualsiasi nodo che comunicherà con **luci**. Per informazioni su come abilitare le porte IP sui nodi del cluster consultare Sezione 2.3.1, «Come abilitare le porte IP sui nodi del cluster».

Per amministrare Red Hat High Availability Add-On con **Conga** installare ed eseguire **luci** nel modo seguente:

1. Selezionare un computer per **luci** ed installare il software **luci** su quel computer. Per esempio:

```
# yum install luci
```

NOTA

Generalmente un computer in una gabbia per server o centro dati è in possesso di **luci**; Tuttavia è possibile implementare **luci** anche su un computer del cluster.

2. Avviare **luci** usando **service luci start**. Per esempio:

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

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

NOTA

Con Red Hat Enterprise Linux release 6.1 è possibile configurare alcuni aspetti del comportamento di **luci** tramite il file **/etc/sysconfig/luci**, inclusi i parametri della porta e dell'host come descritto in Sezione 2.4, «Configurazione di **luci** con **/etc/sysconfig/luci**». I suddetti parametri verranno automaticamente riportati nell'URL all'avvio del servizio **luci**.

3. In un web browser inserire l'URL del server **luci** nell'indirizzo URL e e successivamente selezionare **Vai** (o equivalente). La sintassi dell'URL per il server **luci** è **https://*luci_server_hostname*:*luci_server_port***. Il valore predefinito di *luci_server_port* è **8084**.

   Al primo accesso di **luci** verrà visualizzato un prompt specifico del web browser relativo al certificato SSL autofirmato (del server **luci**). Previa accettazione delle caselle di dialogo, il web browser visualizzerà la pagina di login di **luci**.

4. Anche se qualsiasi utente in grado di eseguire una autenticazione con il sistema che ospita **luci** può effettuare un login con lo stesso **luci**, con Red Hat Enterprise Linux 6.2 solo l'utente root del sistema che esegue **luci** potrà accedere a qualsiasi dei componenti **luci** fino a quando un amministratore (l'utente root o un utente con permessi di amministrazione) imposta i permessi necessari per l'utente in questione. Per informazioni su come impostare i permessi **luci** per gli utenti consultare Sezione 3.3, «Controllo accesso di luci».

   Dopo aver eseguito il login sarà possibile visualizzare la pagina **Homebase** di **luci** come mostrato in Figura 3.1, «Pagina Homebase di luci».

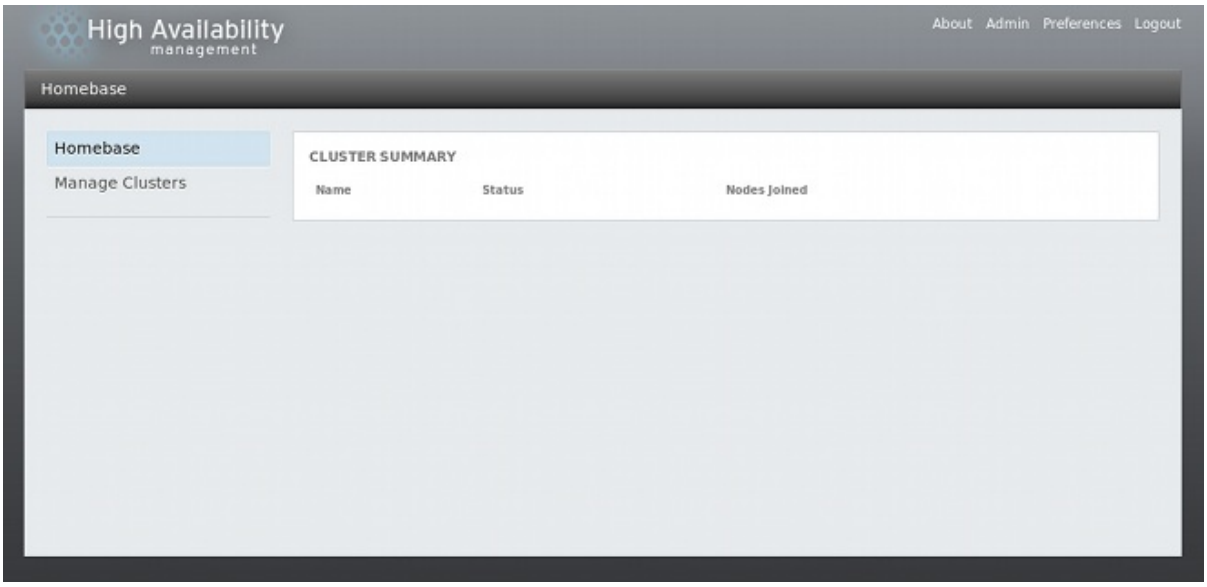


Figura 3.1. Pagina Homebase di luci

NOTA

È presente un timeout di inattività per **luci** che espelle l'utente dopo 15 minuti di inattività.

3.3. CONTROLLO ACCESSO DI LUCI

Dalla release iniziale di Red Hat Enterprise Linux 6 sono state inserite le seguenti funzioni nella pagina **Utenti e Permessi**.

- Con Red Hat Enterprise Linux 6.2, l'utente root o l'utente con permessi amministrativi per **luci** su un sistema che esegue **luci**, è in grado di controllare l'accesso ai rispettivi componenti impostando i permessi per i singoli utenti.
- Con Red Hat Enterprise Linux 6.3, l'utente root o l'utente con permessi amministrativi per **luci**, è in grado di utilizzare l'interfaccia **luci** per aggiungere gli utenti al sistema.
- Con Red Hat Enterprise Linux 6.4, l'utente root o l'utente con permessi amministrativi per **luci**, è in grado di utilizzare l'interfaccia **luci** per cancellare gli utenti dal sistema.

Per aggiungere e cancellare utenti o per impostare i rispettivi permessi, eseguire un login su **luci** come utente **`root`** o come utente al quale sono stati precedentemente conferiti i permessi amministrativi. Fatto questo selezionare **Ammin** nell'angolo in alto sulla destra della schermata di **luci**. Così facendo sarà possibile visualizzare la pagina **Utenti e Permessi** nella quale possono essere visualizzati gli utenti esistenti.

Per cancellare gli utenti selezionare quelli desiderati e successivamente fare clic sul pulsante **`Cancella selezionati`**.

Per aggiungere un utente selezionare **`Aggiungi un utente`** ed inserire il nome desiderato.

Per impostare o modificare i permessi di un utente, selezionate l'utente dal menu a tendina in **Permessi utente**. A questo punto sarà possibile impostare i seguenti permessi:

`Amministratore di Luci`

Conferisce all'utente gli stessi permessi di un utente root, con permessi completi su tutti i cluster insieme alla possibilità di impostare o rimuovere i permessi stessi a tutti gli altri utenti ad eccezione dell'utente root.

`È possibile creare i Cluster`

Permette all'utente di creare nuovi cluster, come descritto in Sezione 3.4, «Creazione di un cluster».

`È possibile importare i cluster esistenti`

Permette all'utente di aggiungere un cluster esistente all'interfaccia di **luci** come descritto in Sezione 4.1, «Aggiungere un cluster esistente all'interfaccia di luci».

Per ogni cluster creato o importato su **luci**, sarà possibile impostare i seguenti permessi per l'utente indicato:

`È possibile visualizzare questo Cluster`

Permette all'utente di visualizzare il cluster specializzato.

`È possibile modificare la configurazione del cluster`

Permette all'utente di modificare la configurazione per il cluster specificato ma non di aggiungere e rimuovere i nodi del cluster.

`È possibile abilitare, disabilitare, riposizionare, e migrare i gruppi di servizi`

Permette all'utente di gestire i servizi ad elevata disponibilità come descritto in Sezione 4.5, «Gestione servizi ad elevata disponibilità».

`È possibile arrestare, avviare o riavviare i nodi del cluster`

Permette all'utente di gestire i nodi di un cluster come descritto in Sezione 4.3, «Gestione dei nodi del cluster».

È possibile aggiungere e cancellare i nodi

Permette ad un utente di aggiungere e cancellare i nodi di un cluster come descritto in Sezione 3.4, «Creazione di un cluster».

È possibile rimuovere questo cluster da Luci

Permette ad un utente di rimuovere un cluster dall'interfaccia di **luci** come descritto in Sezione 4.4, «Avvio, arresto, rimozione e riavvio del cluster».

Selezionare **Invia** per implementare i permessi o **Resetta** per tornare ai valori iniziali.

3.4. CREAZIONE DI UN CLUSTER

Per creare un cluster con **luci** specificare il nome di un cluster, aggiungere i nodi al cluster, inserire le password per **ricci** di ogni nodo ed inviare la richiesta di creazione del cluster. Se le informazioni relative alle password ed al nodo sono corrette **Conga** installerà automaticamente il software nei nodi (se i pacchetti software appropriati non sono installati) e successivamente avvierà il cluster. Creare un cluster nel modo seguente:

1. Selezionare **Gestisci cluster** dal menu nella parte sinistra della pagina **luci Homebase**. A questo punto apparirà la schermata **Cluster** come riportato in Figura 3.2, «Pagina di gestione del cluster di luci».

Figura 3.2. Pagina di gestione del cluster di luci

2. Selezionate **Crea**. A questo punto verrà visualizzata la schermata **Crea nuovo Cluster** come mostrato in Figura 3.3, «casella di dialogo per la creazione del cluster di luci» .

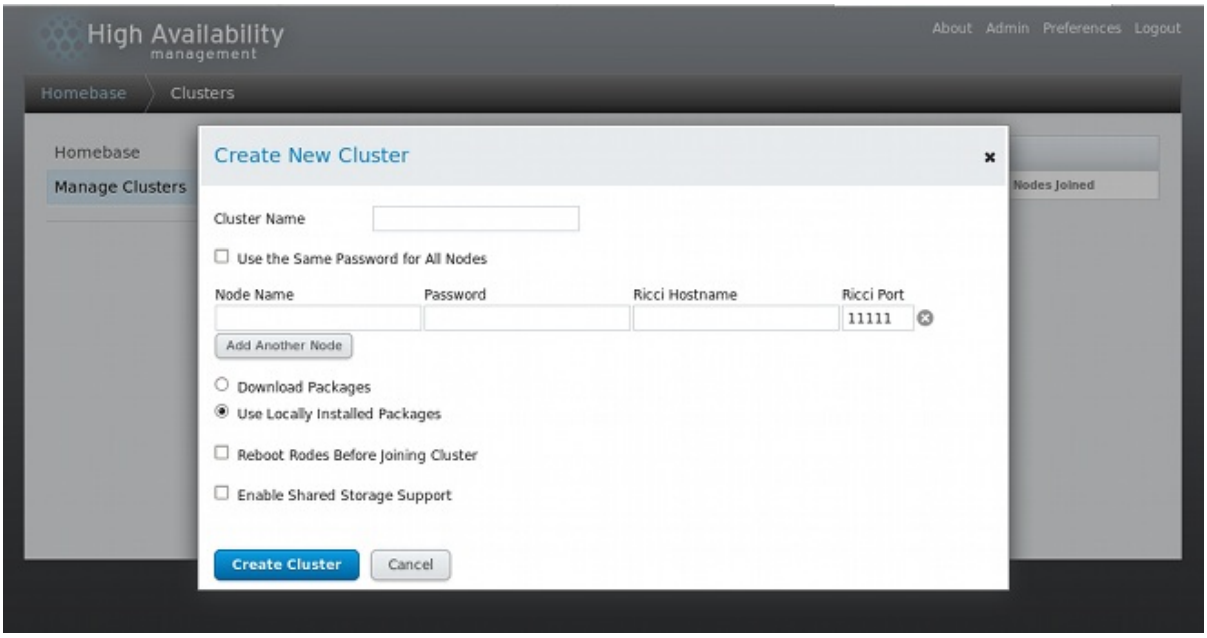


Figura 3.3. casella di dialogo per la creazione del cluster di luci

3. Inserire i seguenti parametri sulla schermata **Crea nuovo Cluster**:

   - Nel campo **Nome del cluster** inserire il nome del cluster. Il nome non può superare i 15 caratteri.

   - Se ogni nodo nel cluster ha la stessa password di **ricci** sarà possibile selezionare **Usa la stessa password per tutti i nodi** per riempire automaticamente il campo **password** durante l'aggiunta dei nodi.

   - Inserire il nome per un nodo del cluster nella colonna **Nome del nodo** e la password di **ricci** nella colonna **Password**.

   - Se il sistema è configurato con una rete privata apposita usata solo per il traffico del cluster allora configurate **luci** per una comunicazione con **ricci** su un indirizzo diverso da quello risolto dal nome del nodo del cluster. Per fare questo inserie l'indirizzo come **Hostname di Ricci**.

   - Se usate una porta diversa per l'agente **ricci** allora l'impostazione predefinita è 11111. Questo parametro può essere modificato.

   - Selezionare **Aggiungi un altro nodo** ed inserire il nome del nodo e la password di **ricci** per ogni nodo aggiuntivo nel cluster.

   - Se non desiderate aggiornare i pacchetti software del cluster precedentemente installati sui nodi alla creazione del cluster, lasciate l'opzione **Usa i pacchetti installati localmente** selezionata. Se desiderate aggiornare tutti i pacchetti software del cluster selezionate l'opzione **Scarica pacchetti**.

NOTA

Se selezionate **Usa i pacchetti installati localmente** o l'opzione **Scarica pacchetti**, se qualsiasi componente del cluster risulta mancante (**cman**, **`rgmanager`**, **`modcluster`** e le rispettive dipendenze), essa verrà installata. Se non possono essere installate la creazione del nodo fallirà.

- Selezionare **Riavvia i nodi prima di unirli al cluster**.
- Selezionate **Abilita supporto dello storage condiviso** per l'uso dello storage clusterizzato; Così facendo verranno scaricati i pacchetti che supportano lo storage clusterizzato e verrà altresì abilitato LVM clusterizzato. Eseguite questa selezione quando avrete accesso al Resilient Storage Add-On o Scalable File System Add-On.

4. Selezionate **`Crea cluster`**. Selezionando **`Crea cluster`** verranno eseguite le seguenti azioni:

   1. Se avete selezionato **Scarica pacchetti** i pacchetti software del cluster verranno scaricati sui nodi.
   2. Il software del cluster sarà installato sui nodi (o verrà verificata l'installazione dei pacchetti software corretti).
   3. Il file di configurazione del cluster viene aggiornato e diffuso su ogni nodo nel cluster.
   4. I nodi aggiunti si uniscono al cluster.

   A questo punto è possibile visualizzare un messaggio il quale indica la creazione del cluster. Quando il cluster è pronto la schermata mostrerà lo stato del cluster appena creato come riportato in Figura 3.4, «Visualizzazione dei nodi del cluster». Da notare che se **ricci** non è in esecuzione la creazione del cluster fallirà.

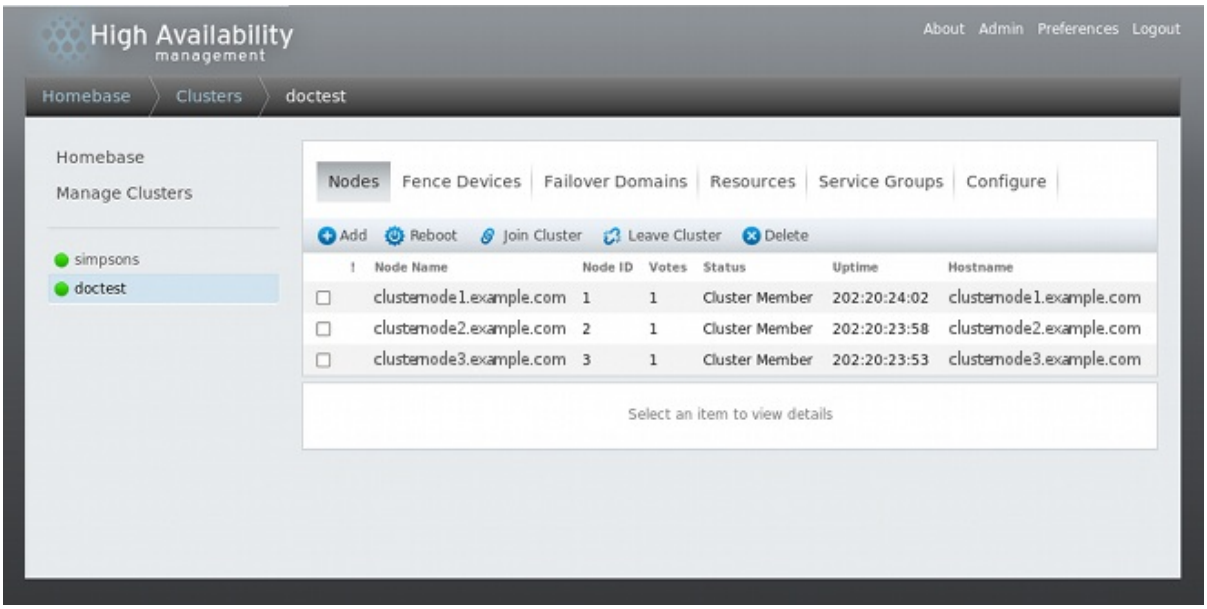
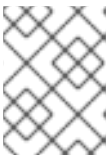


Figura 3.4. Visualizzazione dei nodi del cluster

5. Dopo aver selezionato **`Crea cluster`** per la creazione del cluster, sarà possibile aggiungere o rimuovere i nodi selezionando le funzioni **Aggiungi** o **Rimuovi** dal menu nella parte alta delle pagina di visualizzazione dei nodi. Se non cancellate un intero cluster sarà necessario prima arrestare i nodi e successivamente cancellarli. Per informazioni su come rimuovere un nodo da un cluster esistente in funzione consultare Sezione 4.3.4, «Rimozione di un membro da un cluster».



NOTA

La rimozione di un nodo del cluster è un processo distruttivo e, una volta eseguito, non può essere annullato.

3.5. PROPRIETÀ GLOBALI DEL CLUSTER

Quando selezionate un cluster da configurare verrà visualizzata una pagina specifica al cluster stesso. La suddetta pagina fornisce una interfaccia per la configurazione delle proprietà relative. Per la configurazione di queste proprietà selezionate **Configura** nella parte alta. Così facendo potrete visualizzare le seguenti schede: **Generale**, **Demone di fencing**, **Rete**, **Ring ridondante**, **QDisk** e **Registrazione**. Per poter configurare i parametri seguire le fasi nelle sezioni relative. Se non desiderate configurare parametri specifici ad una scheda, saltate la sezione relativa alla scheda in questione.

3.5.1. Configurazione proprietà generali

Selezionando la scheda **Generali** sarà possibile visualizzare la pagina **Proprietà generali** la quale fornisce una interfaccia per la modifica della versione della configurazione.

- La casella di dialogo **Nome del cluster** mostra il nome del cluster; Questa casella non accetta alcuna modifica del nome. L'unico modo per modificare il nome di un cluster è quello di creare una nuova configurazione con un nuovo nome.
- Il valore **Versione della configurazione** è impostato per impostazione predefinita su **`1`** e viene aumentato automaticamente ogni qualvolta la configurazione del cluster viene modificata. Tuttavia se desiderate impostare un valore diverso specificate un valore nella casella **Versione della configurazione**.

Se avete modificato la **Versione della configurazione** fate clic su **`Applica`** per implementare la modifica.

3.5.2. Configurazione proprietà del demone di fencing

Selezionando **Demone di fencing** sarà possibile visualizzare la pagina **Proprietà del demone di fencing** che fornisce una interfaccia per la configurazione di **Post fail delay** e **Post join delay**. I valori configurati per questi parametri sono generalmente proprietà di fencing per il cluster. Per configurare i dispositivi di fencing specifici per i nodi del cluster usare il menu **Dispositivi di fencing** del cluster come descritto in Sezione 3.6, «Configurazione del dispositivo di fencing».

- Il parametro **Post fail delay** rappresenta il periodo d'attesa in secondi del demone di fencing (**`fenced`**) prima di isolare un nodo (un membro del dominio di fencing) dopo il suo fallimento. Il valore predefinito del **Post fail delay** è **`0`**. Il valore può essere modificato per soddisfare le prestazioni di rete e del cluster.
- Il parametro **Post join delay** rappresenta il periodo d'attesa in secondi del demone di fencing (**`fenced`**) prima di isolare un nodo dopo che il nodo si è unito al demone. Il valore predefinito di **Post Join Delay** è **`6`**. Una impostazione tipica per **Post Join Delay** va dai 20 ai 30 secondi, ma può essere modificato per soddisfare le prestazioni di rete e del cluster.

Inserire i valori necessari e selezionare **`Applica`** per implementare le modifiche.

NOTA

Per maggiori informazioni su **Post join delay** e **Post fail delay**, consultare la pagina man di fenced(8).

3.5.3. Configurazioni di rete

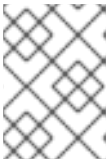
Selezionando **Rete** sarà possibile visualizzare la pagina **Configurazione di rete** la quale fornisce una interfaccia per la configurazione del tipo di trasporto di rete.

Usare questa scheda per selezionare una delle seguenti opzioni:

- **UDP multicast ed opzione Lascia al cluster scegliere l'indirizzo multicast**

  Questa è l'impostazione predefinita. Con questa opzione selezionata il software Red Hat High Availability Add-On creerà un indirizzo multicast in base all'ID del cluster. Esso genererà i 16 bit più bassi dell'indirizzo aggiungendoli alla sezione superiore dell'indirizzo in base al tipo di protocollo IP, se IPV4 o IPV6:

  - Per IPV4 — L'indirizzo formato è 239.192. più i 16 bit più bassi generati dal software Red Hat High Availability Add-On.
  - Per IPV6 — L'indirizzo formato è FF15:: più i 16 bit più bassi generati dal software Red Hat High Availability Add-On.

  NOTA

  L'ID del cluster è un identificatore unico che **cman** genera per ogni cluster. Per visualizzare l'ID del cluster eseguire **`cman_tool status`** sul nodo di un cluster.

- **UDP multicast ed opzione Specifica manualmente l'indirizzo multicast**

  Se desiderate usare un indirizzo multicast specifico selezionare questa opzione per inserire un indirizzo multicast nella casella di testo **Indirizzo Multicast**.

  Se specificate un indirizzo multicast usare la serie 239.192.x.x (o FF15:: per IPv6) usata da **cman**. In caso contrario l'uso di un indirizzo multicast al di fuori della suddetta gamma potrebbe causare risultati non attesi. Per esempio, usando 224.0.0.x ("Tutti gli host sulla rete") potrebbe non essere instradato correttamente oppure non instradato affatto da alcuni hardware.

  Se specificate o modificate un indirizzo multicast sarà necessario riavviare il cluster per implementare le modifiche. Per informazioni su come avviare o arrestare un cluster con **Conga** consultare Sezione 4.4, «Avvio, arresto, rimozione e riavvio del cluster».

  NOTA

  Se specificate un indirizzo multicast assicuratevi di controllare la configurazione dei router usati per il passaggio dei pacchetti del cluster. Alcuni router impiegano una quantità di tempo maggiore per gli indirizzi impattando negativamente sulle prestazioni del cluster.

- **UDP Unicast (UDPU)**

  Con Red Hat Enterprise Linux 6.2 i nodi di un cluster possono comunicare tra loro usando un meccanismo di trasporto UDP Unicast. Tuttavia è consigliato l'uso di un P multicasting per la rete del cluster. UDP Unicast rappresenta una alternativa da usare quando l'IP multicasting non è disponibile. Per implementazioni GFS2 non è consigliato usare UDP Unicast.

Selezionare **`Applica`**. Dopo la modifica del tipo di trasporto sarà necessario riavviare il servizio per implementare le modifiche.

3.5.4. Configurazione Protocollo ring ridondante

Con Red Hat Enterprise Linux 6.4, Red Hat High Availability Add-On rende disponibile il supporto per la configurazione del protocollo ring ridondante. Durante l'uso del suddetto protocollo è consigliato considerare un certo numero di fattori come riportato in Sezione 7.6, «Configurazione Protocollo ring ridondante».

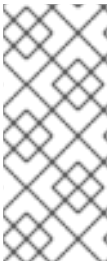
Selezionando **Ring ridondante** potrete visualizzare la pagina **Configurazione protocollo ring ridondante**. Questa pagina mostra tutti i nodi attualmente configurati per il cluster. Se configurate un sistema per poter usare il protocollo ring ridondante, specificate il **Nome alternativo** per ogni nodo del secondo ring.

La pagina **Configurazione protocollo ring ridondante** permette facoltativamente di specificare un **Indirizzo multicast del ring alternativo**, la **Porta CMAN alternativa del ring** ed il **Multicast Packet TTL del ring alternativo** per il secondo ring.

Se specificate un indirizzo multicast per il secondo ring, l'indirizzo o la porta alternativi devono essere diversi dall'indirizzo multicast per il primo ring. Se specificate una porta alternativa i numeri della porta del primo ring e del secondo ring devono differire di almeno due unità poichè il sistema utilizza un valore porta e porta-1 per eseguire le operazioni necessarie. Se non specificate alcun indirizzo alternativo per il secondo ring, il sistema userà automaticamente un indirizzo multicast diverso.

3.5.5. Configurazione del Quorum Disk

Selezionando **QDisk** potrete visualizzare la pagina **Configurazione del Quorum Disk** la quale fornisce una interfaccia per la configurazione dei parametri del quorum disk per un eventuale suo utilizzo.



NOTA

I parametri euristici e quelli relativi al quorum-disk dipendono dall'ambiente del sito e dai requisiti speciali necessari. Per comprendere l'utilizzo dei parametri euristici e di quelli del quorum-disk consultate la pagina man di qdisk(5). Se avete bisogno di assistenza nella comprensione e nell'uso del quorum-disk contattate un rappresentante autorizzato di Red Hat.

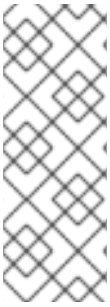
Per impostazione predefinita il parametro **Non usare un Quorum Disk** è abilitato. Se desiderate utilizzare un quorum disk selezionate **Usa un Quorum Disk**, inserite i parametri relativi e successivamente selezionate **`Applica`** e riavviate il cluster per implementare le modifiche.

Tabella 3.1, «Parametri Quorum-Disk» descrive i parametri del quorum disk.

Tabella 3.1. Parametri Quorum-Disk

Parametro	Descrizione
Specifica il dispositivo fisico: Per etichetta del dispositivo	Specifica l'etichetta del quorum disk creata dall'utilità **`mkqdisk`**. Se si utilizza questo campo il demone del quorum legge **`/proc/partitions`** e controlla le presenza delle firme qdisk su ogni dispositivo a blocchi trovato, confrontando l'etichetta con quella specificata. Tale comportamento è utile nelle configurazioni dove il nome del dispositivo del quorum differisce tra i nodi.

Parametro	Descrizione
Euristici	**Percorso per il programma** — Il programma usato per determinare se questo valore euristico è disponibile. Può essere un valore qualsiasi eseguibile da **`/bin/sh -c`**. Un valore 0 indica un successo; qualsiasi altro valore indica un errore. Questo campo è obbligatorio. **Intervallo** — La frequenza (in secondi) alla quale si consulta il valore euristico. L'intervallo predefinito per ogni euristico è 2 secondi. **Risultato** — Il peso di questo euristico. Fare molta attenzione nel determinare i risultati per gli euristici. Il risultato predefinito per ogni euristico è 1. **TKO** — Il numero di errori consecutivi prima di poter dichiarare questo euristico non disponibile.
Risultato totale minimo	Il risultato minimo per un nodo per essere considerato "vivo". Se omesso o impostato su 0, viene usata la funzione predefinita, **`floor((`*`n`*`+1)/2)`**, dove *n* è la somma dei risultati euristici. Il valore del **Risultato totale minimo** non deve mai superare la somma dei risultati euristici; in caso contrario il quorum disk non potrà essere disponibile.



NOTA

Selezionando **Applica** sulla scheda **Configurazione del QDisk** le modifiche al file di configurazione del cluster (**`/etc/cluster/cluster.conf`**) verranno diffuse su ogni nodo del cluster. Tuttavia per il funzionamento del quorum-disk o per implementare qualsiasi modifica effettuata su di esso sarà necessario riavviare il cluster (consultare Sezione 4.4, «Avvio, arresto, rimozione e riavvio del cluster». A tal proposito assicuratevi di aver riavviato il demone **`qdiskd`** su ogni nodo.

3.5.6. Configurazione di login

Selezionando la scheda **Login** sarà possibile visualizzare la pagina **Configurazione login** la quale fornisce una interfaccia per la configurazione delle impostazioni di login.

È possibile configurare le seguenti impostazioni per una configurazione del login globale:

- La selezione di **Registra i messaggi per il debug** abilita i messaggi di debug nel file di log.
- Selezionando **Registra i messaggi su syslog** verranno abilitati i messaggi su **`syslog`**. È possibile selezionare **Funzione messaggi di syslog** e **Priorità messaggi di syslog**. L'impostazione **Priorità messaggi di syslog** indica che i messaggi di un livello selezionato o di un livello più alto saranno inviati a **`syslog`**.
- Selezionando **Registra i messaggi sul file di log** verranno abilitati i messaggi sul file di log. È possibile specificare il nome del **Percorso del file di log**. L'impostazione **Priorità messaggi di**

logfile indica che i messaggi sul livello selezionato o di un livello più elevato saranno scritti sul file di log.

È possibile sovrascrivere le impostazioni di login globale per demoni specifici selezionando uno dei demoni elencati sotto l'intestazione **Override dei login specifici al demone** nella parte bassa della pagina **Configurazione di login**. Dopo la selezione di un demone sarà possibile verificare se registrare i messaggi di debug per quel particolare demone. Sarà possibile specificare altresì le impostazioni del file di log e di **`syslog`** per il demone in questione.

Selezionare **`Applica`** per implementare le modifiche relative alla configurazione di login.

3.6. CONFIGURAZIONE DEL DISPOSITIVO DI FENCING

Il processo di configurazione dei dispositivi di fencing consiste nella creazione, aggiornamento e rimozione dei dispositivi di fencing per il cluster. È necessario configurare i dispositivi di fencing in un cluster prima di poter configurare il fencing dei nodi.

Per creare un dispositivo di fencing selezionare un tipo di dispositivo ed inserire i parametri necessari (ad esempio il nome, indirizzo IP, login e password). Per aggiornare un dispositivo di fencing selezionare un dispositivo e modificarne i parametri. Per la rimozione selezionate il dispositivo desiderato e rimuovetelo.

Questa sezione fornisce le procedure per i seguenti compiti:

- Creazione dei dispositivi di fencing — Consultare la Sezione 3.6.1, «Creazione di un dispositivo di fencing». Una volta creato e conferito un nome al dispositivo di fencing sarà possibile configurare i dispositivi per ogni nodo presente nel cluster come descritto in Sezione 3.7, «Configurazione del processo di fencing per i membri del cluster».
- Aggiornamento dei dispositivi di fencing — Consultare la Sezione 3.6.2, «Modifica di un dispositivo di fencing».
- Rimozione dei dispositivi di fencing — Consultare la Sezione 3.6.3, «Rimozione di un dispositivo di fencing».

Dalla pagina del cluster configurare i dispositivi di fencing per il cluster desiderato selezionando **Dispositivi di fencing** nella parte alta della schermata. Così facendo saranno visualizzati i dispositivi di fencing per il cluster ed il menu per la configurazione del dispositivo: **Aggiungi** e **Cancella**. Questo è il punto di partenza di ogni procedura descritta nelle sezioni seguenti.

NOTA

Se questa è una configurazione iniziale del cluster, nessun dispositivo di fencing è stato creato e quindi non sarà visualizzato alcun dispositivo.

Figura 3.5, «Pagina di configurazione dei dispositivi di fencing di luci» mostra la schermata di configurazione dei dispositivi di fencing prima della creazione di qualsiasi dispositivo.

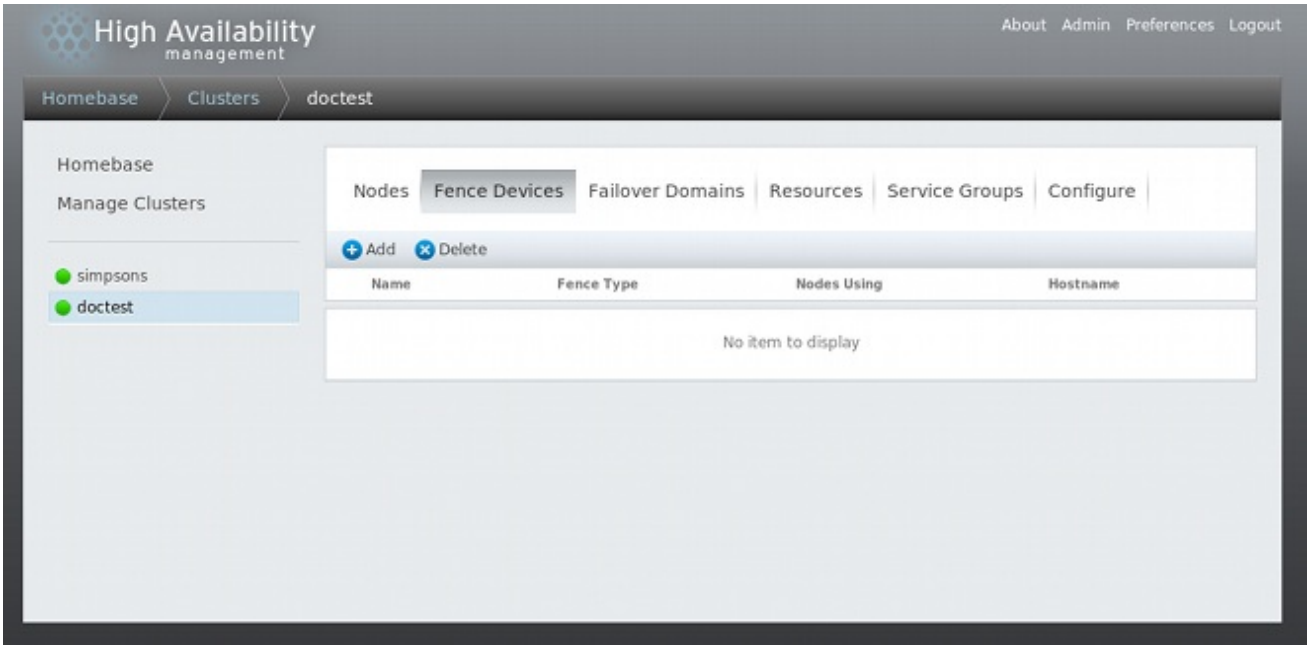


Figura 3.5. Pagina di configurazione dei dispositivi di fencing di luci

3.6.1. Creazione di un dispositivo di fencing

Per creare un dispositivo di fencing seguire le fasi di seguito indicate:

1. Dalla pagina di configurazione **Dispositivi di fencing** selezionare **Aggiungi**. Dopo la selezione di **Aggiungi** sarà visualizzata la casella di dialogo **`Aggiungi dispositivo per il fencing (istanza)`**. Da questo menu a tendina selezionare il tipo di dispositivo di fencing da configurare.

2. Specificare le informazioni nella casella di dialogo **`Aggiungi dispositivo di fencing (istanza)`** in base al tipo di dispositivo. Consultate Appendice A, *Parametri del dispositivo di fencing* per maggiori informazioni sui parametri per il dispositivo di fencing. In alcuni casi sarà necessario specificare i parametri specifici del nodo per il dispositivo di fencing come descritto in Sezione 3.7, «Configurazione del processo di fencing per i membri del cluster».

3. Selezionare **`Invia`**.

Dopo aver aggiunto il dispositivo di fencing esso verrà visualizzato sulla pagina di configurazione dei **Dispositivi di fencing**.

3.6.2. Modifica di un dispositivo di fencing

Per modificare un dispositivo di fencing seguire le fasi di seguito riportate:

1. Dalla pagina di configurazione **Dispositivi di fencing** selezionare il nome del dispositivo da modificare. Così facendo verrà visualizzata la casella di dialogo relativa con i valori configurati per il dispositivo.

2. Per modificare il dispositivo inserire le modifiche desiderate ai parametri visualizzati. Consultare Appendice A, *Parametri del dispositivo di fencing* per maggiori informazioni.

3. Selezionare **`Applica`** ed attendere l'aggiornamento della configurazione.

3.6.3. Rimozione di un dispositivo di fencing

NOTA

I dispositivi di fencing usati non potranno essere cancellati. Per rimuovere un dispositivo usato dal nodo aggiornare la configurazione relativa al fencing per ogni nodo che utilizza il dispositivo e successivamente cancellare il dispositivo interessato.

Per cancellare un dispositivo di fencing seguire le fasi riportate:

1. Dalla pagina di configurazione **Dispositivi di fencing** selezionare la casella relativa ai dispositivi di fencing per la selezione dei dispositivi da cancellare.

2. Fate clic su **`Cancella`** ed attendere l'aggiornamento della configurazione. A questo punto verrà visualizzato un messaggio il quale indica i dispositivi cancellati.

Dopo aver aggiornato la configurazione i dispositivi cancellati non saranno più visualizzati nella schermata.

3.7. CONFIGURAZIONE DEL PROCESSO DI FENCING PER I MEMBRI DEL CLUSTER

Dopo aver completato le fasi iniziali per la creazione di un cluster e dei dispositivi di fencing sarà necessario configurare il processo di fencing per i nodi del cluster. Per configurare tale processo dopo aver creato un nuovo cluster e configurato i dispositivi di fencing per il cluster stesso, seguite le fasi riportate in questa sezione. Da notare che sarà necessario configurare il fencing per ogni nodo del cluster.

Le seguenti sezioni riportano le procedure per la configurazione di un dispositivo di fencing per un nodo, per la configurazione di un nodo con un dispositivo di fencing di backup, e la configurazione di un nodo con alimentazione ridondante:

- Sezione 3.7.1, «Configurazione di un dispositivo di fencing singolo per un nodo»
- Sezione 3.7.2, «Configurazione di un dispositivo di fencing di backup»
- Sezione 3.7.3, «Configurazione di un nodo con alimentazione ridondante»

3.7.1. Configurazione di un dispositivo di fencing singolo per un nodo

Usare la seguente procedura per configurare un nodo con un dispositivo di fencing singolo.

1. Dalla pagina specifica del cluster sarà possibile configurare il fencing per i nodi presenti nel cluster selezionando **Nodi** nella parte alta della schermata. Qui verranno visualizzati i nodi che compongono il cluster. Questa è anche la pagina predefinita visualizzata quando si seleziona il nome del cluster in **Gestisci Cluster** dal menu nella parte sinistra nella pagina **Homebase** di **luci**.

2. Fate clic sul nome del nodo. Selezionando il link sarà possibile visualizzare la pagina relativa alla configurazione del nodo.

   La pagina specifica al nodo mostra qualsiasi servizio in esecuzione sul nodo stesso, insieme ai domini di failover dei quali il nodo è membro. Sarà possibile modificare un dominio di failover esistente selezionandone il nome. Per informazioni sulla configurazione dei domini di failover consultare Sezione 3.8, «Configurazione di un dominio di failover».

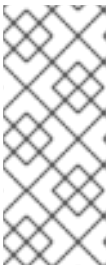
3. Sulla pagina specifica del nodo, sotto **Dispositivi di fencing**, selezionate **`Aggiungi un metodo di fencing`**. Così facendo sarà possibile visualizzare la casella di dialogo **`Aggiungi un metodo di fencing al nodo`**.

4. Inserire un **Nome metodo** relativo al metodo di fencing per questo nodo. Questo rappresenta un nome arbitrario che sarà usato da Red Hat High Availability Add-On. Il nome non sarà uguale al nome DNS per il dispositivo.

5. Selezionare **`Invia`**. Così facendo verrà visualizzata la schermata relativa al nodo nella quale sarà presente il metodo appena aggiunto in **Dispositivi di fencing**.

6. Configurare una istanza per il fencing per questo metodo selezionando **`Aggiungi una istanza per il fencing`**. Così facendo verrà visualizzato un menu a tendina **Aggiungi dispositivo di fencing (Instanza)** dal quale sarà possibile selezionare un dispositivo precedentemente configurato come descritto in Sezione 3.6.1, «Creazione di un dispositivo di fencing».

7. Selezionare un dispositivo di fencing per questo metodo. Se il dispositivo ha bisogno di una configurazione dei parametri specifici del nodo la schermata mostrerà i parametri da configurare. Per informazioni sui suddetti parametri consultare Appendice A, *Parametri del dispositivo di fencing*.



NOTA

Per metodi di fencing non-power (SAN/storage) **Unfencing** è selezionato per impostazione predefinita sulla schermata dei parametri specifici al nodo. Cosi facendo un nodo isolato non verrà riabilitato fino a quando non verrà eseguito prima il riavvio. Per maggiori informazioni su come riabilitare un nodo consultare la pagina man di **`fence_node`**(8).

8. Selezionare **`Invia`**. Così facendo verrete riportati sulla schermata specifica del nodo nella quale sarà possibile visualizzare il metodo e l'instanza per il fencing.

3.7.2. Configurazione di un dispositivo di fencing di backup

È possibile definire metodi multipli di fencing per un nodo. Se il processo di fencing fallisce usando il primo metodo il sistema cercherà di isolare il nodo usando il secondo metodo, seguito da qualsiasi altro metodo aggiuntivo configurato.

Usare la seguente procedura per configurare un dispositivo di fencing di backup per il nodo.

1. Usare la procedura presente in Sezione 3.7.1, «Configurazione di un dispositivo di fencing singolo per un nodo» per configurare il metodo di fencing primario per un nodo.

2. Sotto la schermata per il metodo primario definito selezionare **`Aggiungi metodo di fencing`**.

3. Inserire un nome per il metodo di fencing di backup configurato per questo nodo e selezionare **`Invia`**. Così facendo verrà visualizzata la schermata relativa al nodo con il metodo da voi appena aggiunto sotto al metodo di fencing primario.

4. Configurare una istanza per il fencing per questo metodo selezionando **`Aggiungi una istanza per il fencing`**. Così facendo verrà visualizzato un menu a tendina dal quale sarà possibile selezionare un dispositivo precedentemente configurato come descritto in Sezione 3.6.1, «Creazione di un dispositivo di fencing».

5. Selezionare un dispositivo di fencing per questo metodo. Se il dispositivo ha bisogno di una configurazione dei parametri specifici del nodo la schermata mostrerà i parametri da configurare. Per informazioni sui suddetti parametri consultare Appendice A, *Parametri del dispositivo di fencing*.

6. Selezionare **`Invia`**. Così facendo verrete riportati sulla schermata specifica del nodo nella quale sarà possibile visualizzare il metodo e l'instanza per il fencing.

Continuate ad aggiungere i metodi di fencing in base alle vostre necessità. Sarà possibile modificare l'ordine dei metodi di fencing che saranno usati da questo nodo selezionando **Sposta su** e **Sposta giù**.

3.7.3. Configurazione di un nodo con alimentazione ridondante

Se il cluster è stato configurato con alimentazione ridondante per i nodi assicuratevi di configurare il metodo di fencing in modo tale che i nodi siano stati completamente arrestati al momento di essere isolati. Se configurate ogni sorgente di alimentazione come metodo di fencing separato, ogni sorgente di alimentazione verrà isolata separatamente; il secondo sorgente permetterà al sistema di continuare la sua esecuzione quando il primo è isolato, in questo modo il sistema non verrà mai isolato. Per configurare un sistema con alimentazione doppia è necessario configurare i dispositivi di fencing in modo tale che entrambi i sorgenti di alimentazione siano stati disabilitati ed il sistema completamente disattivato. Durante la configurazione del sistema usando **Conga** tale processo richiederà la configurazione di due istanze all'interno di un unico metodo di fencing.

Per configurare il metodo di fencing di un nodo con alimentazione doppia seguire le fasi riportate in questa sezione.

1. Prima di poter configurare il fencing di un nodo con alimentazione ridondante è necessario configurare ogni interruttore di alimentazione come dispositivo di fencing per il cluster. Per informazioni sulla configurazione dei dispositivi di fencing consultare Sezione 3.6, «Configurazione del dispositivo di fencing».

2. Dalla pagina specifica del cluster selezionate **Nodi** nella parte alta della schermata. Qui verranno visualizzati i nodi che compongono il cluster. Questa è anche la pagina predefinita visualizzata quando si seleziona il nome del cluster in **Gestisci Cluster** dal menu nella parte sinistra nella pagina **Homebase** di **luci**.

3. Fate clic sul nome del nodo. Selezionando il link sarà possibile visualizzare la pagina relativa alla configurazione del nodo.

4. Sulla pagina specifica del nodo selezionate **`Aggiungi metodo di fencing`**.

5. Inserire un nome per il metodo di fencing che state configurando per questo nodo.

6. Selezionare **`Invia`**. Così facendo verrà visualizzata la schermata relativa al nodo nella quale sarà presente il metodo appena aggiunto in **Dispositivi di fencing**.

7. Configurare il primo sorgente di alimentazione come istanza per il fencing di questo metodo selezionando **`Aggiungi una istanza per il fencing`**. Così fancendo verrà visualizzato un menu a tendina dal quale sarà possibile selezionare uno dei dispositivi di fencing precedentemente configurato come descritto in Sezione 3.6.1, «Creazione di un dispositivo di fencing».

8. Selezionare uno dei dispositivi di fencing di questo metodo ed inserire i parametri appropriati per questo dispositivo.

9. Selezionare **Invia**. Così facendo verrete riportati sulla schermata specifica del nodo nella quale sarà possibile visualizzare il metodo e l'instanza per il fencing.

10. Nello stesso metodo di fencing per il quale avete configurato il primo dispositivo selezionare **Aggiungi una istanza per il fencing**. Così facendo visualizzerete un menu a tendina dal quale sarà possibile selezionare il secondo dispositivo di fencing precedentemente configurato come descritto in Sezione 3.6.1, «Creazione di un dispositivo di fencing».

11. Selezionate il secondo dispositivo per questo metodo ed inserite i parametri appropriati per questo dispositivo.

12. Fate clic su **Invia**. Così facendo sarete riportati sulla schermata relativa ai metodi ed alle istanze di fencing, la quale mostra che ogni dispositivo disalimenterà ed alimenterà il sistema in sequenza. Tale procedura viene riportata in Figura 3.6, «Configurazione del fencing con alimentazione doppia».

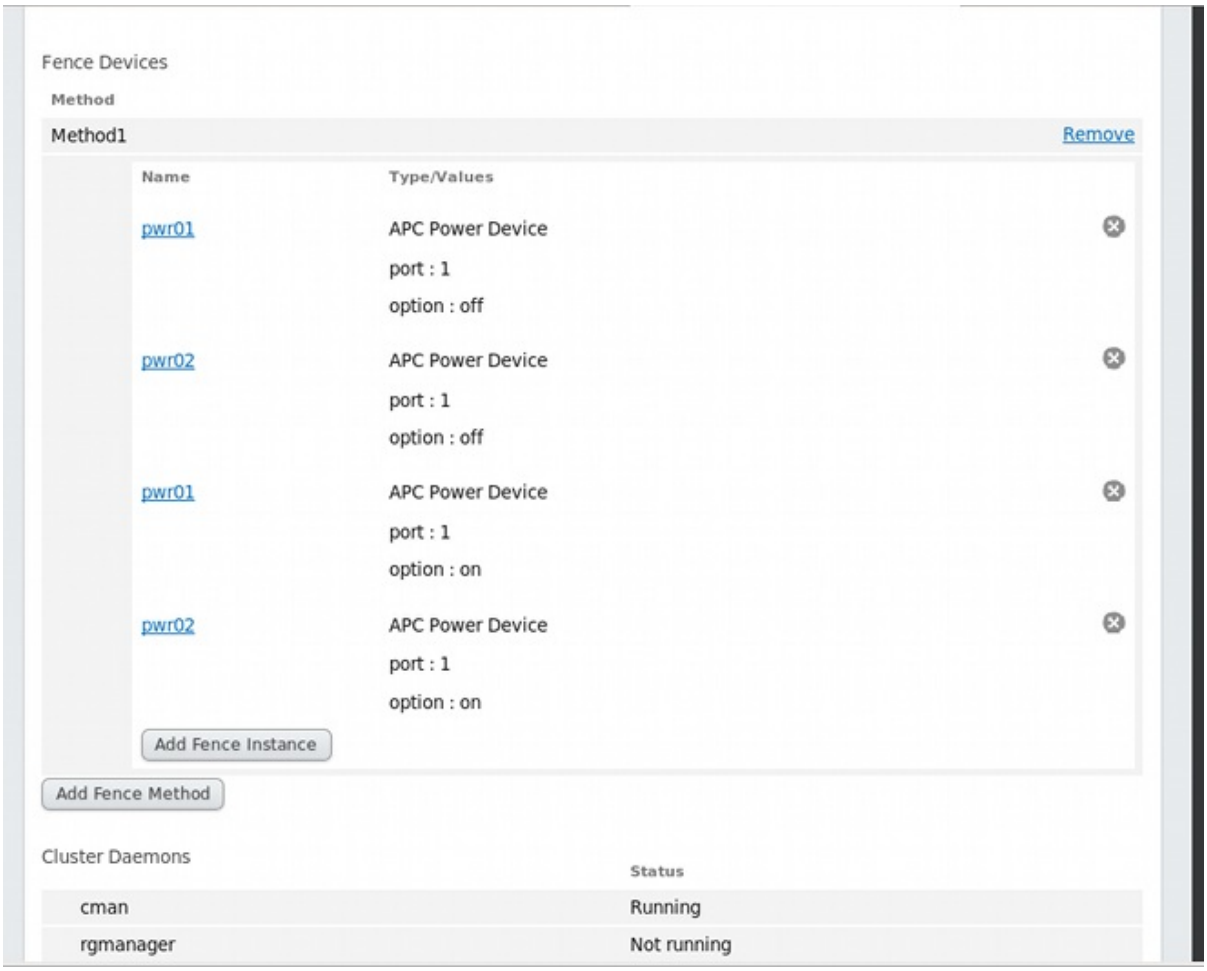


Figura 3.6. Configurazione del fencing con alimentazione doppia

3.8. CONFIGURAZIONE DI UN DOMINIO DI FAILOVER

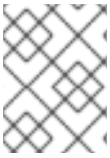
Un dominio di failover è un insieme specifico di nodi del cluster in grado di eseguire un servizio in presenza di un nodo fallito. Il dominio di failover può avere le seguenti caratteristiche:

- Unrestricted — Permette all'utente di specificare un insieme di membri preferiti e di indicare altresì che un servizio del cluster assegnato a questo dominio può essere eseguito su qualsiasi membro disponibile.

- Restricted — Permette all'utente di limitare i membri in grado di eseguire un servizio particolare. Se nessuno dei membri di un dominio di failover limitato è disponibile, il servizio non potrà essere avviato (sia manualmente che dal software del cluster).
- Unordered — Quando un servizio viene assegnato ad un dominio di failover non ordinato, il membro sul quale il servizio viene eseguito verrà selezionato dal gruppo di membri disponibili nel dominio di failover senza seguire alcuna priorità.
- Ordered — Permette all'utente di specificare un ordine preferito tra i membri di un dominio di failover. Il membro che occupa la parte più alta dell'elenco è quello preferito seguito dal secondo membro e così via.
- Failback — Permette all'utente di specificare se un servizio in un dominio di failover deve essere passato sul nodo sul quale era in esecuzione originariamente prima del suo fallimento. La configurazione di questa funzione è utile in casi in cui un nodo fallisce ripetutamente ed è parte di un dominio di failover ordinato. In tal caso se un nodo è il nodo preferito in un dominio di failover sarà possibile passare il servizio tra il nodo preferito ed un altro nodo. Questa impostazione impatta negativamente sulle prestazioni.

NOTA

La caratteristica di failback è applicabile solo se è stato configurato il failover ordinato.



NOTA

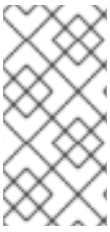
La modifica della configurazione di un dominio di failover non ha alcun effetto sui servizi attualmente in esecuzione.

NOTA

I domini di failover *non* sono necessari per un normale funzionamento.

Per impostazione predefinita i domini di failover non sono limitati ne ordinati.

In un cluster con numerosi membri l'uso di un dominio di failover limitato potrebbe ridurre il compito per l'impostazione del cluster per l'esecuzione di un servizio (come ad esempio **`httpd`**), il quale necessita di una impostazione identica della configurazione su tutti i membri che eseguono il servizio del cluster. Al posto di impostare l'intero cluster in modo da eseguire il servizio sarà necessario impostare solo i membri nel dominio di failover limitato associati con il servizio del cluster.



NOTA

Per configurare un membro preferito creare un dominio di failover non limitato che comprende un solo membro del cluster. Così facendo il servizio del cluster verrà eseguito principalmente sul membro (il membro preferito), permettendo anche di eseguire il failover del servizio del cluster su qualsiasi altro membro.

Le seguenti sezioni descrivono come aggiungere, modificare e rimuovere un dominio di failover.

- Sezione 3.8.1, «Come aggiungere un dominio di failover»
- Sezione 3.8.2, «Come modificare un dominio di failover»

- Sezione 3.8.3, «Rimozione del dominio di failover»

3.8.1. Come aggiungere un dominio di failover

Per aggiungere un dominio di failover seguire le fasi riportate in questa sezione.

1. Dalla pagina del cluster configurare i domini di failover per il cluster in questione selezionando **Domini di failover** nella parte alta della schermata. Così facendo saranno visualizzati i domini di failover configurati per questo cluster.

2. Selezionare **Aggiungi**. Dopo la selezione di **Aggiungi** sarà visualizzata la casella di dialogo **`Aggiungi domini di failover al cluster`** come mostrato in Figura 3.7, «Casella di dialogo di configurazione del dominio di failover di luci».

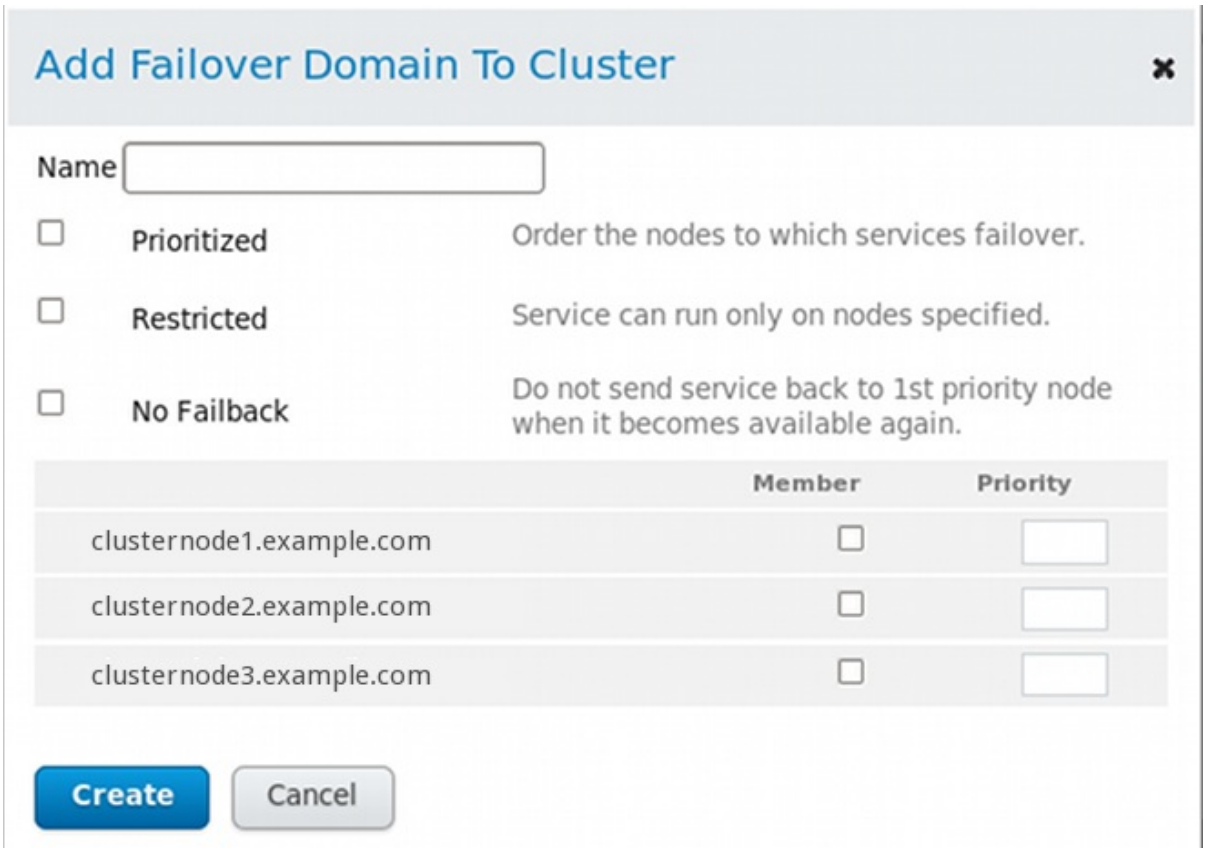
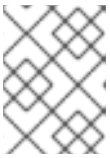


Figura 3.7. Casella di dialogo di configurazione del dominio di failover di luci

3. Nella finestra **`Aggiungi dominio di failover al cluster`** specificare il nome di un dominio di failover nella casella **Nome**.



NOTA

Il nome deve essere sufficientemente descrittivo in modo da distinguere il suo scopo da altri nomi usati nel cluster.

4. Per abilitare l'impostazione della priorità del failover dei membri nel dominio di failover selezionate la casella **Con priorità**. Dopo aver selezionato la casella **Con priorità** sarà possibile impostare il valore **Priorità** per ogni nodo selezionato come membro del dominio di failover.

5. Per limitare il failover ai membri in questo dominio di failover selezionare la casella **Limitato**. Dopo aver selezionato la casella **Limitato** i servizi assegnati a questo dominio di failover verranno spostati solo sui nodi presenti in questo dominio.

6. Per indicare che un nodo non esegue il failback in questo dominio di failover selezionare la casella **No Failback**. Dopo aver selezionato la casella **No Failback** se un servizio viene spostato da un nodo preferito il servizio non verrà spostato sul nodo originale una volta ripristinato.

7. Configurare i membri per questo dominio di failover. Selezionare la casella **Membro** per ogni nodo designato come membro del diminio di failover. Se la casella **Con priorità** è stata selezionata impostare il valore di priorità con la casella **Priorità** per ogni membro del dominio di failover.

8. Selezionate **`Crea`**. Così facendo visualizzerete la pagina **`Domini di failover`** con al suo interno il dominio di failover appena creato. Un messaggio indica che un nuovo dominio è stato creato. Ricaricare la pagina per ottenere lo stato aggiornato.

3.8.2. Come modificare un dominio di failover

Per modificare un dominio di failover seguire le fasi di questa sezione.

1. Dalla pagina del cluster configurare i Domini di failover per il cluster in questione selezionando **Domini di failover** nella parte alta della schermata. Così facendo saranno visualizzati i domini di failover configurati per questo cluster.

2. Selezionare il nome di un dominio di failover. Così facendo visualizzerete la pagina di configurazione per il dominio di failover relativo.

3. Per modificare le impostazioni **Con priorità**, **Limitato**, o **No Failback** del dominio di failover selezionare o deselezionare la casella corrispondente alla proprietà e successivamente **`Aggiorna proprietà`**.

4. Per modificare l'appartenenza al dominio di failover selezionate o deselezionate la casella corrispondente al membro del cluster. Se il dominio di failover presenta una priorità, sarà possibile modificare le impostazioni di priorità del membro del cluster. A questo punto selezionare **`Aggiorna impostazioni`**.

3.8.3. Rimozione del dominio di failover

Per rimuovere un dominio di failover seguire le fasi presenti in questa sezione.

1. Dalla pagina del cluster configurare i Domini di failover per il cluster in questione selezionando **Domini di failover** nella parte alta della schermata. Così facendo saranno visualizzati i domini di failover configurati per questo cluster.

2. Selezionare la casella per il dominio di failover da rimuovere.

3. Selezionare **Cancella**.

3.9. CONFIGURAZIONE DELLE RISORSE GLOBALI DEL CLUSTER

Sarà possibile configurare le risorse globali utilizzabili da qualsiasi servizio in esecuzione nel cluster e quelle disponibili solo a servizi specifici.

Per aggiungere una risorsa globale del cluster seguire le fasi presenti in questa sezione. È possibile aggiungere una risorsa locale ad un servizio specifico durante la configurazione del servizio come descritto in Sezione 3.10, «Come aggiungere un servizio ad un cluster».

1. Dalla pagina specifica del cluster sarà possibile aggiungere le risorse al cluster selezionando **Risorse** nella parte alta della schermata. Così facendo verranno visualizzate le risorse configurate per quel cluster.

2. Selezionate **Aggiungi**. A questo punto sarà visualizzato il menu a tendina **Aggiungi una risorsa al cluster**.

3. Fate clic sulla casella sotto **Aggiungi una risorsa al cluster** e selezionate il tipo di risorsa da configurare.

4. Inserire i parametri della risorsa per la risorsa che state aggiungendo. Appendice B, *Parametri della risorsa HA* descrive i vari parametri.

5. Fate clic su **`Invia`**. Selezionando **`Invia`** verrete ridirezionati sulla pagina relativa alle **`Risorse`**, la quale conterrà la risorsa aggiunta (insieme ad altre risorse).

Per modificare una risorsa esistente seguire le fasi riportate.

1. Dalla pagina **Risorse** di **luci** selezionare il nome della risorsa da modificare. Così facendo visualizzerete i parametri della risorsa interessata.

2. Modificare i parametri della risorsa.

3. Selezionate **`Applica`**.

Per cancellare una risorsa esistente eseguire le seguenti fasi.

1. Dalla pagina **Risorse** di **luci** selezionare la casella della risorsa da rimuovere.

2. Selezionare **Cancella**.

3.10. COME AGGIUNGERE UN SERVIZIO AD UN CLUSTER

Per aggiungere un servizio al cluster seguire le fasi di questa sezione.

1. Dalla pagina specifica del cluster sarà possibile aggiungere i servizi al cluster selezionando **Gruppi di servizi** nella parte alta della schermata del cluster. A questo punto potrete visualizzare i servizi configurati per il cluster. (Dalla pagina **Gruppi di servizi** sarà altresì possibile avviare, riavviare o disabilitare un servizio come descritto in Sezione 4.5, «Gestione servizi ad elevata disponibilità».)

2. Selezionare **Aggiungi**. Così facendo verrà visualizzata la casella di dialogo **Aggiungi gruppo di servizi al cluster**.

3. Sulla casella **`Aggiungi gruppo di servizi al cluster`**, nel campo **Nome del servizio** inserire il nome del servizio.

NOTA

Il nome deve essere sufficientemente descrittivo da distinguere il servizio da altri servizi nel cluster.

4. Selezionare la casella **Avvia automaticamente questo servizio** se desiderate che il servizio si avvii automaticamente all'avvio ed esecuzione del cluster. Se la casella *no* è stata selezionata il servizio dovrà essere avviato manualmente ogni qualvolta il cluster viene avviato.

5. Selezionare la casella **Esegui come esclusivo** per impostare una politica con la quale il servizio viene eseguito su di un nodo sul quale non sono eseguiti altri servizi.

6. Se avete configurato i domini di failover per il cluster sarà possibile utilizzare il menu a tendina del parametro **Dominio di Failover** per selezionare un dominio di failover per questo servizio. Per informazioni sulla configurazione dei domini di failover consultare la Sezione 3.8, «Configurazione di un dominio di failover».

7. Usare la casella **Politica di ripristino** per selezionare la politica di ripristino del servizio. Le opzioni sono **Relocate**, **Restart**, **Restart-Disable** o **Disable** il servizio.

   Selezionando **Restart** il sistema cercherà di riavviare il servizio fallito prima di riposizionare il servizio stesso. Con **Relocate** il sistema dovrà provare a riavviare il servizio in un altro nodo. Selezionando l'opzione **Disable** verrà indicato al sistema di disabilitare il gruppo di risorse se qualsiasi componente fallisce. **Restart-Disable** indica al sistema di riavviare il servizio fallito ma se il riavvio fallisce il servizio sarà disabilitato e non verrà riposizionato su nessun host del cluster.

   Se selezionate **Restart** o **Restart-Disable** come politica di ripristino del servizio, sarà possibile specificare il numero massimo di fallimenti prima di eseguire il riposizionamento o disabilitare il servizio, e l'arco di tempo, espresso in secondi, dopo il quale non eseguire più alcun processo di riavvio.

8. Per aggiungere una risorsa al servizio selezionare **`Aggiungi una risorsa`**. La selezione di **`Aggiungi una risorsa`** causa la visualizzazione di un menu a tendina **`Aggiungi una risorsa al servizio`** il quale permetterà di aggiungere una risorsa globale esistente o di aggiungerne una nuova disponibile *solo* a questo servizio.

   - Per aggiungere una risorsa globale selezionare il nome della risorsa esistente dalla casella **`Aggiungi una risorsa al servizio`**. In questo modo sarà possibile visualizzare la risorsa insieme ai suoi parametri sulla pagina **Gruppi di servizi** per il servizio che state configurando. Per informazioni su come aggiungere o modificare le risorse globali consultare Sezione 3.9, «Configurazione delle risorse globali del cluster»).

   - Per aggiungere una nuova risorsa disponibile solo a questo servizio selezionare il tipo di risorsa da configurare dalla casella **`Aggiungi una risorsa al servizio`**, ed inserire i parametri. Appendice B, *Parametri della risorsa HA* descrive i parametri della risorsa.

   - Durante l'aggiunta di una risorsa al servizio, sia essa una risorsa globale esistente o una risorsa disponibile solo ad un servizio, sarà possibile specificare se la risorsa è un **Albero secondario indipendente** o una **Risorsa non-critica**.

     Se una risorsa risulta essere un albero secondario indipendente, al verificarsi di un errore solo la risorsa interessata verrà riavviata (e non tutto il servizio) prima che il sistema possa eseguire un ripristino normale. È possibile specificare il numero massimo di tentativi di riavvio per una risorsa prima di implementare la politica di ripristino per il servizio. Inoltre sarà possibile specificare la durata del periodo, in secondi, dopo il quale il sistema implementerà la politica di ripristino per il servizio.

     Se una risorsa risulta essere non-critica, al verificarsi di un errore solo la risorsa interessata verrà riavviata e se l'errore persiste solo la risorsa sarà disabilitata e non tutto il servizio. È possibile specificare il numero massimo di tentativi di riavvio per una risorsa prima di

disabilitarla. Inoltre sarà possibile specificare la durata del periodo, in secondi, dopo il quale il sistema disabiliterà la risorsa in questione.

9. Se desiderate aggiungere le risorse figlio alla risorsa che state definendo selezionate **Aggiungi una risorsa figlio**. Selezionando **Aggiungi una risorsa figlio** potrete visualizzare la casella **Aggiungi un risorsa al servizio** dalla quale sarà possibile aggiungere una risorsa globale esistente o aggiungerne una nuova disponibile solo a questo servizio. Se necessario continuate ad aggiungere le risorse figlio alla risorsa in modo da soddisfare i vostri requisiti.

NOTA

Se aggiungete una risorsa del servizio Samba collegare direttamente la risorsa al servizio e *non* come figlio ad un'altra risorsa.

10. Se avete terminato di aggiungere le risorse al servizio, e completato l'aggiunta delle risorse figlio alle risorse, selezionate **Invia**. Selezionando **Invia** verrete indirizzati sulla pagina **Gruppi di servizi** la quale mostrerà il servizio aggiunto (insieme ad altri servizi).

NOTA

Per verificare l'esistenza della risorsa del servizio IP usata in un servizio del cluster, usare il comando **/sbin/ip addr show** su un nodo del cluster (al posto del comando **ifconfig**). Il seguente output mostra il comando **/sbin/ip addr show** eseguito su un nodo che esegue il servizio del cluster:

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

Per modificare un servizio esistente eseguire le seguenti fasi.

1. Dalla casella di dialogo **Gruppi di servizi** selezionare il nome del servizio da modificare. Così facendo verranno visualizzati i parametri e le risorse configurate per quel servizio.

2. Modificare i parametri del servizio.

3. Selezionare **Invia**.

Per cancellare uno o più servizi esistenti eseguire le seguenti fasi.

1. Dalla pagina **luci Gruppi di servizi** selezionare la casella corrispondente al servizio da cancellare.

2. Selezionare **Cancella**.

3. Con Red Hat Enterprise Linux 6.3 sarà possibile visualizzare un messaggio di conferma per la rimozione dei gruppi di servizi o gruppi, i quali arrestano le risorse interessate, prima che **luci** possa cancellare qualsiasi servizio. Selezionare **Cancella** per chiudere la casella di dialogo senza rimuovere alcun servizio, o selezionare semplicemente **Procedi** per rimuovere i servizi selezionati.

CAPITOLO 4. GESTIONE DI RED HAT HIGH AVAILABILITY ADD-ON CON CONGA

Questo capitolo descrive i vari compiti amministrativi per la gestione di Red Hat High Availability Add-On e consiste nelle seguenti sezioni:

- Sezione 4.1, «Aggiungere un cluster esistente all'interfaccia di luci»
- Sezione 4.2, «Rimozione di un cluster dall'interfaccia di luci»
- Sezione 4.3, «Gestione dei nodi del cluster»
- Sezione 4.4, «Avvio, arresto, rimozione e riavvio del cluster»
- Sezione 4.5, «Gestione servizi ad elevata disponibilità»
- Sezione 4.6, «Backup e ripristino della configurazione di luci»

4.1. AGGIUNGERE UN CLUSTER ESISTENTE ALL'INTERFACCIA DI LUCI

Se avete precedentemente creato un cluster High Availability Add-On sarà possibile aggiungere il cluster all'interfaccia di **luci** in modo da poterlo gestire con **Conga**.

Per aggiungere un cluster esistente all'interfaccia di **luci** seguire le seguenti fasi:

1. Selezionare **Gestisci cluster** dal menu sulla sinistra della pagina **Homebase** di **luci**. A questo punto verrà visualizzata la schermata **Cluster**.
2. Selezionare **Aggiungi**. Sarà possibile ora visualizzare **Aggiungi un cluster esistente**.
3. Inserire l'hostname del nodo e la password di **ricci** per qualsiasi nodo presente nel cluster. Poichè ogni nodo contiene tutte le informazioni sulla configurazione per il cluster, ciò dovrebbe fornire informazioni sufficienti per poter aggiungere il cluster all'interfaccia di **luci**.
4. Selezionare **`Connetti`**. La schermata **Aggiungi un cluster esistente** mostra il nome del cluster ed i nodi restanti al suo interno.
5. Inserire le password di **ricci** per ogni nodo nel cluster oppure inserire una sola password e selezionare **Usa la stessa password per tutti i nodi**.
6. Fare clic su **`Aggiungi cluster`**. Il cluster precedentemente configurato verrà ora visualizzato sulla schermata **Gestisci cluster**.

4.2. RIMOZIONE DI UN CLUSTER DALL'INTERFACCIA DI LUCI

È possibile rimuovere un cluster dalla GUI di gestione di **luci** senza interessare i servizi del cluster o la sua appartenenza. Se rimuovete un cluster sarà possibile, se desiderato, aggiungerlo nuovamente. È possibile eseguire tale operazione anche per aggiungere il cluster su una nuova istanza di **luci** come descritto in Sezione 4.1, «Aggiungere un cluster esistente all'interfaccia di luci».

Per rimuovere un cluster esistente dalla GUI di gestione di **luci** senza interessare i servizi del cluster o la sua appartenenza seguire le seguenti fasi:

1. Selezionare **Gestisci cluster** dal menu sulla sinistra della pagina **Homebase** di **luci**. A questo punto verrà visualizzata la schermata **Cluster**.
2. Selezionare il cluster che desiderate rimuovere.
3. Selezionare **Rimuovi**.

Per informazioni sulla rimozione completa di un cluster, l'arresto di tutti i servizi, e la rimozione delle informazioni sulla configurazione dai nodi consultare Sezione 4.4, «Avvio, arresto, rimozione e riavvio del cluster».

4.3. GESTIONE DEI NODI DEL CLUSTER

Questa sezione riporta il metodo attraverso il quale eseguire le funzioni di gestione dei nodi con il componente del server **luci** di **Conga**:

- Sezione 4.3.1, «Riavvio di un nodo del cluster»
- Sezione 4.3.2, «Esclusione o inserimento di un nodo nel cluster»
- Sezione 4.3.3, «Come aggiungere un membro ad un cluster in esecuzione»
- Sezione 4.3.4, «Rimozione di un membro da un cluster»

4.3.1. Riavvio di un nodo del cluster

Per riavviare un nodo nel cluster eseguire le seguenti fasi:

1. Dalla pagina specifica del cluster selezionate **Nodi** nella parte alta della schermata. Qui verranno visualizzati i nodi che compongono il cluster. Questa è anche la pagina predefinita visualizzata quando si seleziona il nome del cluster in **Gestisci Cluster** dal menu nella parte sinistra nella pagina **Homebase** di **luci**.
2. Selezionare il nodo da riavviare facendo clic sulla casella per il nodo corrispondente.
3. Selezionare **Riavvia** dal menu nella parte alta della pagina. Così facendo il nodo selezionato verrà riavviato e sarà possibile visualizzare un messaggio nella parte alta della pagina il quale indica che il nodo è stato riavviato.
4. Ricaricate la pagina per visualizzare lo stato aggiornato del nodo.

È altresì possibile riavviare più di un nodo per volta selezionando tutti i nodi da riavviare prima di selezionare **Riavvia**.

4.3.2. Esclusione o inserimento di un nodo nel cluster

È possibile usare il componente del server **luci** di **Conga** per escludere un nodo dal cluster attivo arrestando tutti i servizi sul nodo interessato. Allo stesso modo potrete usare il componente del server **luci** di **Conga** per inserire nuovamente un nodo all'interno del cluster.

L'esclusione di un nodo dal cluster non rimuoverà le informazioni di configurazione del cluster dal nodo in questione; inoltre il nodo stesso apparirà ancora all'interno della schermata dei nodi del cluster con uno stato **`Non membro del cluster`**. Per informazioni su come rimuovere il nodo dalla configurazione del cluster consultare Sezione 4.3.4, «Rimozione di un membro da un cluster».

Per poter escludere un nodo dal cluster eseguire le fasi di seguito riportate. Così facendo arresterete il software del cluster nel nodo. L'esclusione di un nodo dal cluster impedirà al nodo di unirsi automaticamente al cluster al momento del riavvio.

1. Dalla pagina specifica del cluster selezionate **Nodi** nella parte alta della schermata. Qui verranno visualizzati i nodi che compongono il cluster. Questa è anche la pagina predefinita visualizzata quando si seleziona il nome del cluster in **Gestisci Cluster** dal menu nella parte sinistra nella pagina **Homebase** di **luci**.

2. Selezionate il nodo desiderato facendo clic sulla casella corrispondente al nodo.

3. Selezionare la funzione **Abbandona il cluster** dal menu nella parte alta della pagina. Così facendo verrà visualizzato un messaggio che indicherà l'arresto del nodo.

4. Ricaricate la pagina per visualizzare lo stato aggiornato del nodo.

Sarà possibile escludere più di un nodo per volta selezionando tutti i nodi desiderati prima di fare clic su **Abbandona il cluster**.

Per poter riammettere i nodi nel cluster selezionare i nodi desiderati tramite le caselle corrispondeti e successivamente **Unisci al cluster**. Così facendo i nodi si uniranno al cluster e permetterà ai nodi stessi di far parte del cluster al momento del riavvio.

4.3.3. Come aggiungere un membro ad un cluster in esecuzione

Per aggiungere un membro ad un cluster in esecuzione seguire le fasi in questa sezione.

1. Dalla pagina specifica del cluster selezionate **Nodi** nella parte alta della schermata. Qui verranno visualizzati i nodi che compongono il cluster. Questa è anche la pagina predefinita visualizzata quando si seleziona il nome del cluster in **Gestisci Cluster** dal menu nella parte sinistra nella pagina **Homebase** di **luci**.

2. Selezionare **Aggiungi**. Selezionando **Aggiungi** potrete visualizzare la casella **`Aggiungi i nodi al cluster`**.

3. Inserire il nome del nodo nella casella **Hostname del nodo**; inserire la password di **ricci** nella casella **Password**. Se usate una porta diversa per l'agente **ricci** allora l'impostazione predefinita è 11111 modificate questo parametro in base alla porta che state usando.

4. Selezionate **Abilita supporto dello storage condiviso**, così facendo verranno scaricati i pacchetti che supportano lo storage clusterizzato e verrà altresì abilitato LVM clusterizzato. Eseguite questa selezione quando avrete accesso al Resilient Storage Add-On o Scalable File System Add-On.

5. Se desiderate aggiungere altri nodi selezionate **Aggiungi un altro nodo** ed inserire il nome del nodo e la password per ogni nodo aggiuntivo.

6. Selezionare **`Aggiungi nodi`**. La selezione di **`Aggiungi nodi`** causerà le seguenti azioni:

    1. Se avete selezionato **Scarica pacchetti** i pacchetti software del cluster verranno scaricati sui nodi.

    2. Il software del cluster sarà installato sui nodi (o verrà verificata l'installazione dei pacchetti software corretti).

    3. Il file di configurazione del cluster viene aggiornato e diffuso su ogni nodo nel cluster — incluso il nodo aggiunto.

4. Il nodo aggiunto si unisce al cluster.

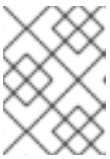
   La pagina **Nodi** apparirà con un messsaggio il quale indica che il nodo è stato aggiunto al cluster. Ricaricate la pagina per aggiornare lo stato.

7. Dopo aver aggiunto il nodo fate clic sul nome del nodo stesso per configurare il fencing, come descritto in Sezione 3.6, «Configurazione del dispositivo di fencing».

4.3.4. Rimozione di un membro da un cluster

Per cancellare un membro da un cluster esistente in esecuzione seguire le fasi di questa sezione. Se non cancellate contemporaneamente tutti i nodi presenti nel cluster ricordate di arrestare i nodi prima di rimuoverli.

1. Dalla pagina specifica del cluster selezionate **Nodi** nella parte alta della schermata. Qui verranno visualizzati i nodi che compongono il cluster. Questa è anche la pagina predefinita visualizzata quando si seleziona il nome del cluster in **Gestisci Cluster** dal menu nella parte sinistra nella pagina **Homebase** di **luci**.

   NOTA

   Per poter eseguire il failover dei servizi dopo la rimozione di un nodo saltate la fase successiva.

2. Disabilitate o riposizionate ogni servizio in esecuzione sul nodo da cancellare. Per informazioni su come disabilitare e riposizionare i servizi consultate la Sezione 4.5, «Gestione servizi ad elevata disponibilità».

3. Selezionate il nodo o i nodi da cancellare.

4. Selezionare **Cancella**. La pagina **`Nodi`** indica che il nodo è stato rimosso. Ricaricate la pagina per visualizzare lo stato corrente.

IMPORTANTE

La rimozione di un nodo del cluster è un processo distruttivo e, una volta eseguito, non può essere annullato.

4.4. AVVIO, ARRESTO, RIMOZIONE E RIAVVIO DEL CLUSTER

È possibile avviare, arrestare e riavviare un cluster eseguendo le seguenti azioni sui singoli nodi presenti nel cluster. Dalla pagina del cluster fare clic su **Nodi** nella parte alta della schermata del cluster. Così facendo visualizzerete i nodi che costituiscono il cluster.

Le operazioni di avvio e di riavvio per i nodi di un cluster permettono di creare piccole interruzioni del servizio che permettono di spostare il servizio stesso su un altro membro del cluster a causa dell'arresto del nodo sul quale era in esecuzione.

Per arrestare un cluster eseguire le seguenti fasi. Così facendo si arresterà il software del cluster nei nodi senza rimuovere le informazioni sulla configurazione del cluster dai nodi in questione; inoltre i nodi stessi appariranno ancora all'interno della schermata dei nodi del cluster con uno stato **`Non membro del cluster`**.

1. Selezionare tutti i nodi nel cluster selezionando le caselle corrispondenti.

2. Selezionare la funzione **Abbandona il cluster** dal menu nella parte alta della pagina. Così facendo verrà visualizzato un messaggio che indicherà l'arresto del nodo.

3. Ricaricate la pagina per visualizzare lo stato aggiornato del nodo.

Per avviare un cluster eseguire le seguenti fasi:

1. Selezionare tutti i nodi nel cluster selezionando le caselle corrispondenti.

2. Selezionare la funzione **Unisci al cluster** dal menu sulla parte superiore della pagina.

3. Ricaricate la pagina per visualizzare lo stato aggiornato del nodo.

Per riavviare un cluster in esecuzione arrestare prima tutti i nodi presenti, successivamente avviare tutti i nodi in un cluster come sopra descritto.

Per cancellare un cluster eseguire le seguenti fasi. Così facendo verranno arrestati tutti i servizi del cluster e rimosse dai nodi le informazioni relative alla configurazione. Non sarà altresì più possibile visualizzare i nodi all'interno della schermata del cluster. Se desiderate in futuro aggiungere un cluster esistente utilizzando uno dei nodi rimossi, **luci** indicherà che il nodo usato non è membro di alcun cluster.

IMPORTANTE

La rimozione di un cluster rappresenta una operazione distruttiva e non sarà possibile ripristinare lo stato precedente a tale operazione. Per ripristinare un cluster sarà necessario creare nuovamente e ridefinire il cluster da zero.

1. Selezionare tutti i nodi nel cluster selezionando le caselle corrispondenti.

2. Selezionare la funzione **Cancella** dal menu sulla parte superiore della pagina.

Se desiderate rimuovere un cluster dall'interfaccia di **luci** senza arresterne i servizi o se desiderate modificare l'appartenenza del cluster, usare l'opzione **Remove** sulla pagina **Gestisci cluster** come descritto in Sezione 4.2, «Rimozione di un cluster dall'interfaccia di luci».

4.5. GESTIONE SERVIZI AD ELEVATA DISPONIBILITÀ

Oltre ad aggiungere e modificare un servizio, come descritto in Sezione 3.10, «Come aggiungere un servizio ad un cluster», sarà possibile eseguire le seguenti funzioni di gestione per i servizi ad elevata disponibilità attraverso il componente del server **luci** di **Conga**:

- Avvio di un servizio
- Riavvio di un servizio
- Disabilitare un servizio
- Rimozione di un servizio
- Riposizionamento di un servizio

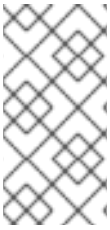
Utilizzando la pagina relativa al cluster sarà possibile gestire i servizi per quel cluster selezionando **Gruppi di servizi** nella sezione superiore della schermata. Così facendo verranno visualizzati i servizi configurati del cluster.

- **Avvio di un servizio** — Per avviare qualsiasi servizio non in esecuzione selezionare i servizi desiderati tramite le caselle relative e successivamente **Avvia**.
- **Riavvio di un servizio** — Per riavviare un servizio in esecuzione selezionare il servizio desiderato tramite la casella corrispondente e successivamente **Riavvia**.
- **Disabilitare un servizio** — Per disabilitare un servizio in esecuzione selezionarlo tramite la casella corrispondente e successivamente selezionare**Disabilita**.
- **Cancellare un servizio** — Per cancellare un servizio non in esecuzione selezionarlo tramite la casella corrispondente e successivamente selezionare **Cancella**.
- **Riposizionare un servizio** — Per riposizionare un servizio in esecuzione selezionare il nome corrispondente nella schermata dei servizi. Così facendo potrete visualizzare la pagina relativa alla configurazione dei servizi, visualizzando altresì su quale nodo il servizio è attualmente in esecuzione.

  Dalla casella **`Avvia sul nodo...`** selezionare il nodo sul quale desiderate riposizionare il servizio e successivamente fate clic sull'icona **Avvia**. A questo punto verrà visualizzato un messaggio nella parte alta della schermata il quale indicherà che il servizio è stato riavviato. Ricaricare la schermata per visualizzare il nuovo stato del servizio, così facendo la schermata indicherà che il servizio è in esecuzione sul nodo selezionato.

NOTA

Se il servizio in esecuzione è un servizio **`vm`**, la casella a tendina mostrerà una opzione **`migra`** al posto di una opzione **`riposiziona`**.



NOTA

È possibile altresì avviare, riavviare, disabilitare o cancellare un servizio selezionando il nome sulla pagina **Servizi**. Così facendo potrete visualizzare la pagina di configurazione del servizio. Nell'angolo destro della pagina di configurazione del servizio sono presenti le stesse icone per **Avvia**, **Riavvia**, **Disabilita**, e **Cancella**.

4.6. BACKUP E RIPRISTINO DELLA CONFIGURAZIONE DI LUCI

Con Red Hat Enterprise Linux 6.2 usare la seguente procedura per un backup del database **luci**, archiviato in **`/var/lib/luci/data/luci.db`**. Esso non rappresenta la configurazione del cluster, archiviata nel file **`cluster.conf`**, ma contiene invece un elenco di utenti, cluster e proprietà associate mantenute da **luci**. Per impostazione predefinita il backup creato da questa procedura verrà salvato sulla stessa directory del file **`luci.db`**.

1. Eseguire **`service luci stop`**.
2. Eseguire **`service luci backup-db`**.

   Facoltativamente è possibile specificare il nome di un file come parametro per il comando **`backup-db`**, il quale a sua volta salverà il database **luci** sul file stesso. Per esempio, per salvare il database **luci** sul file **`/root/luci.db.backup`**, eseguire il comando **`service luci backup-db /root/luci.db.backup`**. Da notare tuttavia che i file di backup scritti in posti diversi da **`/var/lib/luci/data/`** (per backup dei nomi specificati usando il comando **`service luci backup-db`**) non verranno mostrati nell'output del comando **`list-backups`**.

3. Eseguire **`service luci start`**.

Usare la seguente procedura per ripristinare il database di **luci**.

1. Eseguire **`service luci stop`**.
2. Eseguire **`service luci list-backups`** e prendere nota del nome del file da ripristinare.
3. Eseguire **`service luci restore-db /var/lib/luci/data/`*`lucibackupfile`*** dove *lucibackupfile* è il file di backup da ripristinare.

   Per esempio, il seguente comando ripristina le informazioni relative alla configurazione di **luci** archiviate nel file di backup **`luci-backup20110923062526.db`**:

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

4. Eseguire **`service luci start`**.

Se avete bisogno di ripristinare un database di **luci** ma avete perso il file **`host.pem`** dalla macchina sulla quale avete creato il backup a causa di una reinstallazione completa, sarà necessario aggiungere manualmente i cluster su **luci** per poter autenticare nuovamente i nodi.

Usare la seguente procedura per ripristinare il database di **luci** su una macchina diversa da quella sulla quale avete eseguito il backup. Oltre a ripristinare il database sarà necessario copiare il file del certificato SSL per assicurare l'autenticazione di **luci** con i nodi di **ricci**. In questo esempio il backup è stato eseguito sulla macchina **`luci1`** e ripristinato su **`luci2`**.

1. Eseguire i seguenti comandi per creare un backup di **luci** su **`luci1`** e copiare il file del certificato SSL ed il backup di **luci** su **`luci2`**.

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

2. Su **`luci2`**, assicuratevi che **luci** sia stato installato e non sia in esecuzione. Installare il pacchetto se non precedentemente fatto.
3. Eseguire i seguenti comandi per le autenticazioni necessarie e ripristinare il database **luci** da **`luci1`** a **`luci2`**.

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

CAPITOLO 5. CONFIGURAZIONE DI RED HAT HIGH AVAILABILITY ADD-ON CON IL COMANDO CCS

Con Red Hat Enterprise Linux 6.1 e versioni più recenti Red Hat High Availability Add-On fornisce un supporto per il comando per la configurazione del cluster **ccs**. Questo comando permette la creazione, modifica e visualizzazione del file di configurazione del cluster **cluster.conf** da parte di un amministratore. Usare il comando **ccs** per configurare un file di configurazione del cluster su un file system locale o su di un nodo remoto. Utilizzando il comando **ccs** un amministratore sarà in grado di avviare ed arrestare i servizi di un cluster su uno o tutti i nodi in un cluster configurato.

Questo capitolo descrive come configurare il file di configurazione del cluster di Red Hat High Availability Add-On usando il comando **ccs**. Per informazioni su come utilizzare il comando **ccs** per la gestione di un cluster in esecuzione consultare Capitolo 6, *Gestione di Red Hat High Availability Add-On con **ccs***.

Questo capitolo consiste nelle seguenti versioni:

NOTA

Assicuratevi che l'implementazione High Availability Add-On usata sia supportata e soddisfi i requisiti necessari. Consultate un rappresentante di Red Hat per verificare la configurazione prima di implementarla. Implementate altresì un periodo di prova per le varie modalità d'errore.

NOTA

Questo capitolo fa riferimento ad attributi ed elementi **cluster.conf** comunemente usati. Per un elenco completo ed una descrizione degli elementi ed attributi di **cluster.conf**, consultate lo schema disponibile su **/usr/share/cluster/cluster.rng**, **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (per esempio **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

5.1. PANORAMICA OPERATIVA

Questa sezione descrive gli aspetti operativi generali sull'uso del comando **ccs** per configurare un cluster:

- Sezione 5.1.1, «Creazione del file di configurazione del cluster su di un sistema locale»
- Sezione 5.1.2, «Visualizzazione della configurazione corrente del cluster»
- Sezione 5.1.3, «Specificare le password di ricci con il comando ccs»
- Sezione 5.1.4, «Modifica dei componenti della configurazione del cluster»

5.1.1. Creazione del file di configurazione del cluster su di un sistema locale

Utilizzando il comando **ccs** sarà possibile creare un file di configurazione del cluster su di un nodo oppure crearne uno su di un file system locale ed inviarlo ad un host presente nel cluster. Così facendo sarete in grado di lavorare su di un file da una macchina locale dove sarà possibile mantenerlo sotto un meccanismo di controllo della versione oppure usare un tag in base alle vostre esigenze. L'uso del comando **ccs** non necessita di privilegi root.

Quando create e modificate un file di configurazione del cluster su di un nodo usando il comando **ccs**, usare l'opzione **-h** per specificare il nome dell'host. Ciò crea e modifica il file **cluster.conf** sull'host:

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

Per creare e modificare un file di configurazione del cluster su un sistema locale usare l'opzione **-f** del comando **ccs** per specificare il nome del file di configurazione quando eseguite una operazione sul cluster. Il nome è a discrezione dell'utente.

```
ccs -f file [options]
```

Dopo aver creato il file localmente sarà possibile inviarlo su di un nodo usando l'opzione **--setconf** del comando **ccs**. Su una macchina host di un cluster il file da inviare verrà chiamato **cluster.conf** e sarà posizionato nella directory **/etc/cluster**.

```
ccs -h host -f file --setconf
```

Per informazioni su come utilizzare **--setconf** del comando **ccs** consultare Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.1.2. Visualizzazione della configurazione corrente del cluster

Se in qualsiasi momento della creazione di un file di configurazione del cluster desiderate visualizzare il file corrente, usate il seguente comando specificando il nodo nel cluster come host:

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

Se state creando un file di configurazione del cluster su un sistema locale sarà possibile specificare l'opzione **-f** al posto dell'opzione **-h** come descritto in Sezione 5.1.1, «Creazione del file di configurazione del cluster su di un sistema locale».

5.1.3. Specificare le password di ricci con il comando ccs

Per eseguire i comandi **ccs**, i quali distribuiscono copie del file **cluster.conf** ai nodi di un cluster, sarà necessario installare ed eseguire **ricci** sui nodi del cluster come descritto in Sezione 2.13, «Considerazioni su **ricci**». Per la prima interazione con **ricci** da qualsiasi macchina specifica sarà necessario utilizzare una password.

Se non avete inserito una password per l'istanza di **ricci** su una macchina specifica, sarà necessario inserire la password quando richiesto dal comando **ccs**. Alternativamente usare l'opzione **-p** per specificare una password **ricci** sulla linea di comando.

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

Quando inoltrate il file **cluster.conf** su tutti gli altri nodi nel cluster usando l'opzione **--sync** del comando **ccs** ed avete specificato una password **ricci** per il comando, **ccs** potrà utilizzare la password per ogni nodo nel cluster. Se è necessario impostare sui singoli nodi password diverse per **ricci** allora utilizzate il comando **--setconf** con l'opzione **-p** per distribuire su un nodo per volta il file di configurazione.

5.1.4. Modifica dei componenti della configurazione del cluster

Usare il comando **ccs** per configurare i componenti del cluster ed i rispettivi attributi nel file di configurazione del cluster. Dopo aver aggiunto un componente al file per modificare gli attributi dei componenti in questione sarà necessario rimuovere il componente definito ed aggiungerlo nuovamente con gli attributi modificati. Per informazioni su come eseguire questo processo con ogni componente consultare le sezioni individuali di questo capitolo.

Gli attributi del componente del cluster **cman** forniscono una eccezione alla procedura per la modifica dei componenti del cluster. Per modificare questi attributi usare **--setcman** del comando **ccs**, specificando i nuovi attributi. Specificando questa opzione imposterete tutti i valori non specificati esplicitamente sui rispettivi valori predefinititi, come riportato in Sezione 5.1.5, «Comandi che sovrascrivono le impostazioni precedenti».

5.1.5. Comandi che sovrascrivono le impostazioni precedenti

Sono disponibili diverse opzioni del comando **ccs** per la sovrascrittura delle semantiche durante l'impostazione delle proprietà. Ciò significa che sarà possibile usare **ccs** con una di queste opzioni senza specificare le impostazioni, resettando così tutte le impostazioni al proprio valore predefinito. Queste opzioni sono:

- **--settotem**
- **--setdlm**
- **--setrm**

- **--setcman**
- **--setmulticast**
- **--setaltmulticast**
- **--setfencedaemon**
- **--setlogging**
- **--setquorumd**

Per esempio, per resettare tutte le proprietà del demone di fencing eseguire il seguente comando:

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

Da notare tuttavia che se utilizzate uno di questi comandi per resettare una proprietà, le altre proprietà verranno resettate sui rispettivi valori predefiniti. Per esempio, usare il seguente comando per impostare **post_fail_delay** su 5:

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

Dopo aver eseguito il suddetto comando e utilizzate il comando di seguito riportato per impostare **post_join_delay** su 10, **post_fail_delay** verrà impostata sul suo valore predefinito:

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

Per resettare sia **post_fail_delay** che **post_join_delay**, inserirli sullo stesso comando come riportato nel seguente esempio:

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

Per maggiori informazioni sulla configurazione dei dispositivi di fencing. Consultare Sezione 5.5, «Configurazione dei dispositivi di fencing».

5.1.6. Convalida della configurazione

Se utilizzate il comando **ccs** per creare e modificare il file di configurazione del cluster, la configurazione verrà convalidata automaticamente in base allo schema del cluster. Con Red Hat Enterprise Linux 6.3 il comando **ccs** convalida la configurazione in base allo schema **/usr/share/cluster/cluster.rng** sul nodo specificato con l'opzione **-h**. In precedenza il comando **ccs** utilizzava sempre lo schema disponibile con il comando **ccs**, **/usr/share/ccs/cluster.rng** sul sistema locale. Se utilizzate l'opzione **-f** per specificare il sistema locale, **ccs** utilizza lo schema **/usr/share/ccs/cluster.rng** disponibile con il comando **ccs** sul sistema in questione.

5.2. FASI NECESSARIE PER LA CONFIGURAZIONE

Di seguito sono riportate le fasi necessarie per la configurazione del software di Red Hat High Availability Add-On con il comando **ccs**:

1. Assicurarsi che **ricci** sia in esecuzione su tutti i nodi nel cluster. Consultare Sezione 5.3, «Avvio di **ricci**».

2. Creazione di un cluster. Consultare Sezione 5.4, «Creazione di un cluster».
3. Configurazione dei dispositivi di fencing. Consultare Sezione 5.5, «Configurazione dei dispositivi di fencing».
4. Configurazione del processo di fencing per i membri del cluster. Consultare Sezione 5.7, «Configurazione del processo di fencing per i membri del cluster».
5. Creazione di domini di failover. Consultare Sezione 5.8, «Configurazione di un dominio di failover».
6. Creazione di risorse. Consultare Sezione 5.9, «Configurazione delle risorse globali del cluster».
7. Creazione servizi del cluster. Consultare Sezione 5.10, «Come aggiungere un servizio al cluster».
8. Configurazione di un quorum disk se necessario. Consultare Sezione 5.13, «Configurazione di un quorum disk».
9. Configurazione delle proprietà globali del cluster. Consultare Sezione 5.14, «Configurazioni varie del cluster».
10. Inoltro del file di configurazione del cluster a tutti i nodi. Consultare Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.3. AVVIO DI RICCI

Per creare e distribuire i file di configurazione del cluster sui nodi è necessario che il servizio **ricci** sia in esecuzione su ogni nodo. Prima di avviare **ricci** assicurarsi di avere configurato il sistema nel modo seguente:

1. Le porte IP sui nodi del cluster devono essere abilitate per **ricci**. Per maggiori informazioni su come abilitare le porte IP sui nodi del cluster consultare Sezione 2.3.1, «Come abilitare le porte IP sui nodi del cluster».
2. Il servizio **ricci** è installato su tutti i nodi nel cluster ed una password **ricci** è stata assegnata, come descritto in Sezione 2.13, «Considerazioni su **`ricci`**».

Dopo aver installato e configurato **ricci** su ogni nodo avviare il servizio **ricci**:

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

5.4. CREAZIONE DI UN CLUSTER

Questa sezione descrive come creare, modificare e cancellare la struttura della configurazione del cluster usando il comando **`ccs`** senza fencing, domini di failover e servizi HA. Le sezioni seguenti descrivono come configurare le parti interessate della configurazione.

Per creare la struttura del file di configurazione del cluster creare e conferire un nome al cluster e successivamente aggiungere i nodi al suo interno come mostrato nella procedura riportata:

1. Creare un file di configurazione del cluster su uno dei nodi eseguendo il comando **`ccs`** usando il parametro **`-h`** per specificare il nodo sul quale creare il file e l'opzione **`createcluster`** per specificare un nome.

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

Per esempio il seguente comando crea un file di configurazione su **node-01.example.com** chiamato **mycluster**:

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

Il nome del cluster non può superare i 15 caratteri.

Se un file **cluster.conf** esiste già sull'host specificato l'esecuzione di questo comando sostituirà il file esistente.

Se desiderate creare un file di configurazione del cluster su un sistema locale sarà possibile specificare l'opzione **-f** al posto dell'opzione **-h**. Per informazioni su come creare il file localmente consultare Sezione 5.1.1, «Creazione del file di configurazione del cluster su di un sistema locale».

2. Per configurare i nodi contenuti dal cluster eseguire il seguente comando per ogni nodo nel cluster:

```
ccs -h host --addnode node
```

Per esempio i seguenti comandi aggiungono i nodi **node-01.example.com**, **node-02.example.com**, e **node-03.example.com** al file di configurazione su **node-01.example.com**:

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

Per visualizzare un elenco di nodi configurati per un cluster eseguire il seguente comando;

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

Esempio 5.1, «File **cluster.conf** dopo aver aggiunto tre nodi» mostra un file di configurazione **cluster.conf** dopo aver creato un cluster **mycluster** il quale contiene i nodi **node-01.example.com** **node-02.example.com** e **node-03.example.com**.

Esempio 5.1. File `cluster.conf` dopo aver aggiunto tre nodi

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

```
        </fence>
      </clusternode>
    </clusternodes>
    <fencedevices>
    </fencedevices>
    <rm>
    </rm>
</cluster>
```

Quando aggiungete un nodo al cluster sarà possibile specificare il numero di voti conferiti dal nodo per determinare la presenza di un quorum. Per impostare il numero di voti per un nodo del cluster usare il seguente comando:

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

Quando aggiungete un nodo **ccs** assegnerà al nodo stesso un valore intero unico usato come identificatore del nodo. Se desiderate specificare l'identificatore manualmente usate il seguente comando:

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

Per rimuovere un nodo dal cluster eseguite il seguente comando:

```
ccs -h host --rmnode node
```

Una volta terminata la configurazione di tutti i componenti del cluster sarà necessario eseguire la sincronizzazione del file di configurazione del cluster su tutti i nodi come riportato in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.5. CONFIGURAZIONE DEI DISPOSITIVI DI FENCING

Il processo di configurazione dei dispositivi di fencing consiste nella creazione, aggiornamento e rimozione dei dispositivi per il cluster. È necessario creare ed assegnare un nome ai dispositivi di fencing in un cluster prima di poter configurare il fencing dei nodi. Per informazioni su come configurare il fencing dei nodi in un cluster consultare Sezione 5.7, «Configurazione del processo di fencing per i membri del cluster».

Prima di configurare i dispositivi di fencing modificate alcune delle proprietà del demone del vostro sistema rispetto ai valori predefiniti. I valori da configurare per il demone di fencing sono valori generali per il cluster. Le proprietà generali per il fencing interessate sono di seguito riportate:

- **post_fail_delay** rappresenta il periodo di attesa del demone di fencing, espresso in secondi, (**fenced**) prima di isolare un nodo (un membro del dominio del fencing) dopo il suo fallimento. Il valore predefinito di **post_fail_delay** è **0** ma può essere modificato per soddisfare i requisiti di prestazione della rete e del cluster.
- Il parametro **post-join_delay** rappresenta il periodo d'attesa in secondi del demone di fencing (**fenced**) prima di isolare un nodo dopo che il nodo si è unito al demone. Il valore predefinito di **post_join_delay** è **6**. Una impostazione tipica per **post_join_delay** va dai 20 ai 30 secondi, ma può essere modificato per soddisfare le prestazioni di rete e del cluster.

I valori di **post_fail_delay** e **post_join_delay** vengono resettati con l'opzione **--setfencedaemon** del comando **ccs**. Da notare che l'esecuzione del comando **ccs --setfencedaemon** sovrascriverà tutte le proprietà esistenti del demone di fencing esplicitamente impostate, ripristinando i loro valori predefiniti.

Per esempio, per configurare un valore di **post_fail_delay** eseguire il seguente comando. Questo comando sovrascriverà i valori di tutte le altre proprietà del demone di fencing esistenti impostate con il comando in questione, ripristinandone i valori predefiniti.

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

Per configurare un valore di **post_join_delay** eseguire il seguente comando. Questo comando sovrascriverà i valori di tutte le altre proprietà del demone di fencing esistenti impostate con il comando in questione, ripristinandone i valori predefiniti.

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

Per configurare un valore sia per **post_join_delay** che per **post_fail_delay** eseguire il seguente comando:

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

NOTA

Per maggiori informazioni sugli attributi **post_join_delay** e **post_fail_delay** e sulle proprietà aggiuntive del demone di fencing modificabili consultare la pagina man fenced(8) e gli schemi presenti su **/usr/share/cluster/cluster.rng** e **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Per configurare un dispositivo di fencing per un cluster eseguire il seguente comando:

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

Per esempio, per configurare un dispositivo di fencing apc nel file di configurazione su un nodo **node1** chiamato **myfence** con un indirizzo IP **apc_ip_example**, login **login_example**, ed una password **password_example** eseguire il seguente comando:

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

Il seguente esempio mostra la sezione **fencedevices** del file di configurazione **cluster.conf** dopo l'aggiunta del dispositivo di fencing APC:

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

Durante la configurazione dei dispositivi di fencing per un cluster potrebbe essere utile consultare l'elenco dei dispositivi disponibili, le opzioni presenti per ogni dispositivo e l'elenco di dispositivi di

fencing configurati correttamente per il cluster. Per informazioni aggiuntive su come utilizzare il comando **ccs** per stampare un elenco di dispositivi di fencing disponibili, opzioni o un elenco di dispositivi configurati correttamente consultare Sezione 5.6, «Elenco dei dispositivi di fencing ed opzioni».

Per rimuovere un dispositivo di fencing dalla configurazione del cluster eseguire il seguente comando:

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

Per rimuovere un dispositivo di fencing chiamato **myfence** del file di configurazione del cluster sul nodo **node1** eseguire:

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

Se desiderate modificare gli attributi di un dispositivo di fencing precedentemente configurato, rimuovere prima il dispositivo di fencing interessato ed aggiungerlo nuovamente con gli attributi modificati.

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.6. ELENCO DEI DISPOSITIVI DI FENCING ED OPZIONI

Usare il comando **ccs** per stampare un elenco di dispositivi di fencing disponibili e le opzioni relative. È possibile altresì usare il comando **ccs** per stampare un elenco di dispositivi di fencing configurati correttamente per il cluster.

Per stampare un elenco di dispositivi di fencing disponibili per il cluster eseguire il seguente comando:

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

Per esempio il seguente comando elenca i dispositivi di fencing disponibili sul nodo del cluster **node1**, mostrando un output d'esempio.

```
[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
```

Per stampare un elenco di opzioni da specificare per un tipo di fencing particolare usare il seguente comando:

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

Per esempio, il seguente comando elenca le opzioni per il fence agent **`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
```

Per stampare un elenco di dispositivi di fencing disponibili per il cluster eseguire il seguente comando:

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

5.7. CONFIGURAZIONE DEL PROCESSO DI FENCING PER I MEMBRI DEL CLUSTER

Dopo aver completato le fasi iniziali di creazione di un cluster e dei dispositivi di fencing sarà necessario configurare il processo di fencing per i nodi del cluster. Per configurare questo processo dopo la creazione di un nuovo cluster e la configurazione dei dispositivi usati per il fencing, seguite le fasi riportate in questa sezione. Configurare il processo di fencing per ogni nodo del cluster.

Questa sezione documenta le seguenti procedure:

- Sezione 5.7.1, «Configurazione di un dispositivo di fencing singolo basato sull'alimentazione per un nodo»
- Sezione 5.7.2, «Configurazione di un dispositivo singolo di fencing basato sullo storage per un nodo»
- Sezione 5.7.3, «Configurazione di un dispositivo di fencing di backup»
- Sezione 5.7.4, «Configurazione di un nodo con alimentazione ridondante»
- Sezione 5.7.5, «Rimozione dei metodi e delle istanze del fencing»

5.7.1. Configurazione di un dispositivo di fencing singolo basato sull'alimentazione per un nodo

Usare la seguente procedura per configurare un nodo con un dispositivo singolo di fencing basato sull'alimentazione che utilizza un dispositivo chiamato **apc**, il quale a sua volta usa un agente di fencing **fence_apc**.

1. Aggiungere un metodo di fencing per il nodo e specificare un nome.

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

   Per esempio, per configurare un metodo chiamato **APC** per il nodo **node-01.example.com** nel file di configurazione sul nodo del cluster **node-01.example.com**, eseguire il seguente comando:

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

2. Aggiungere una istanza per il metodo. È necessario specificare il dispositivo di fencing da usare per il nodo, il nodo sul quale viene applicata questa istanza, il nome del metodo e qualsiasi opzione specifica al nodo:

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

   Per configurare una istanza di fencing nel file di configurazione sul nodo **node-01.example.com** del cluster il quale utilizza la porta 1 dell'interruttore APC sul dispositivo chiamato **apc** per isolare il nodo **node-01.example.com** usando il metodo **APC**, eseguire il seguente comando:

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

Sarà necessario aggiungere un metodo di fencing per ogni nodo presente nel cluster. I seguenti comandi sono usati per la configurazione di un metodo di fencing per ogni nodo con il metodo **APC**. Il dispositivo per il metodo di fencing specifica **apc** come nome del dispositivo, il quale rappresenta un dispositivo precedentemente configurato con l'opzione **--addfencedev** come descritto in Sezione 5.5,

«Configurazione dei dispositivi di fencing». Ogni nodo viene configurato con un numero di porta unico dell'interruttore APC. Il numero di porta per **node-01.example.com** è **1**, il numero di porta per **node-02.example.com** è **2**, ed il numero di porta per **node-03.example.com** è **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
```

Esempio 5.2, «**cluster.conf** dopo l'aggiunta dei metodi di fencing basati sull'alimentazione» mostra un file di configurazione **cluster.conf** dopo l'aggiunta dei metodi e delle istanze di fencing su ogni nodo del cluster.

Esempio 5.2. cluster.conf dopo l'aggiunta dei metodi di fencing basati sull'alimentazione

```
<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>
```

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.7.2. Configurazione di un dispositivo singolo di fencing basato sullo storage per un nodo

Quando si utilizzano i metodi di fencing di tipo non-power (cioè fencing SAN/storage) per isolare un nodo, sarà necessario configurare *unfencing* per il dispositivo usato per il processo di isolamento. Tale operazione assicura che il nodo isolato non venga riabilitato fino a quando non sarà riavviato. Durante la configurazione di unfencing di un nodo specificare un dispositivo speculare al dispositivo di fencing corrispondente da voi configurato, con l'aggiunta delle azioni **on** o **enable**.

Per maggiori informazioni su come riabilitare un nodo dopo il suo isolamento consultare la pagina man di **fence_node**(8).

Utilizzare la seguente procedura per configurare un nodo con un dispositivo di fencing singolo basato sullo storage il quale utilizza un dispositivo chiamato **sanswitch1** il quale a sua volta usa un agente **fence_sanbox2**.

1. Aggiungere un metodo di fencing per il nodo e specificare un nome.

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

   Per esempio per configurare un metodo di fencing chiamato **SAN** per il nodo **node-01.example.com** nel file di configurazione sul nodo del cluster **node-01.example.com**, eseguire il seguente comando:

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

2. Aggiungere una istanza per il metodo. È necessario specificare il dispositivo di fencing da usare per il nodo, il nodo sul quale viene applicata questa istanza, il nome del metodo e qualsiasi opzione specifica al nodo:

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

   Per configurare una istanza di fencing nel file di configurazione sul nodo **node-01.example.com** del cluster il quale utilizza la porta 11 dell'interruttore SAN sul dispositivo chiamato **sanswitch1** per isolare il nodo **node-01.example.com** usando il metodo **SAN**, eseguire il seguente comando:

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

3. Per configurare unfence per il dispositivo di fencing basato sullo storage su questo nodo eseguire il seguente comando:

   ```
   ccs -h host --addunfence fencedevicename node action=on|off
   ```

Aggiungere un metodo di fencing per ogni nodo del cluster. I seguenti comandi configurano un metodo di fencing per ogni nodo con il metodo **SAN**. Il dispositivo per il metodo di fencing specifica **sanswitch** come il nome del dispositivo, il quale rappresenta un dispositivo precedentemente configurato con

l'opzione --addfencedev come descritto in Sezione 5.5, «Configurazione dei dispositivi di fencing» . Ogni nodo è configurato con un numero di porta fisica SAN unico: Il numero di porta per **node-01.example.com** è **11**, per **node-02.example.com** è **12**, e per **node-03.example.com** è **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
```

Esempio 5.3, «**cluster.conf** dopo l'aggiunta dei metodi di fencing basati sullo storage» mostra un file di configurazione **cluster.conf** dopo aver aggiunto i metodi e le istanze di fencing ed unfencing per ogni nodo presente nel cluster.

Esempio 5.3. `cluster.conf` dopo l'aggiunta dei metodi di fencing basati sullo storage

```
<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>
```

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.7.3. Configurazione di un dispositivo di fencing di backup

È possibile definire metodi multipli di fencing per un nodo. Se il processo di fencing fallisce usando il primo metodo il sistema cercherà di isolare il nodo usando il secondo metodo, seguito da qualsiasi altro metodo aggiuntivo configurato. Per configurare il metodo di backup per il fencing configurare due metodi per un nodo ed una istanza per ogni nodo.

NOTA

L'ordine con il quale il sistema utilizza i metodi di fencing configurati segue l'ordine riportato nel file di configurazione del cluster. Il primo metodo configurato con il comando **ccs** è il metodo primario, il secondo metodo sarà quello di backup. Per modificare l'ordine rimuovere il metodo primario dal file di configurazione per poi aggiungerlo nuovamente.

Sarà possibile stampare in qualsiasi momento un elenco dei metodi e delle istanze di fencing attualmente configurate per un nodo usando il seguente comando. Se non specificate alcun nodo il comando elencherà i metodi e le istanze configurate per tutti i nodi.

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

Usare la seguente procedura per configurare un nodo con un metodo di fencing primario che utilizza un dispositivo chiamato **apc**, il quale a sua volta usa un agente di fencing **fence_apc**, ed un dispositivo di fencing di backup che utilizza **sanswitch1**, con un agente **fence_sanbox2**. Poichè il dispositivo **sanswitch1** è un agente di fencing basato sullo storage sarà necessario configurare unfencing per quel dispositivo.

1. Aggiungere un metodo di fencing primario per il nodo conferendone un nome.

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

   Per esempio, per configurare un metodo chiamato **APC** come metodo primario per il nodo **node-01.example.com** nel file di configurazione sul nodo del cluster **node-01.example.com**, eseguire il seguente comando:

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

2. Aggiungere una istanza di fencing per il metodo primario. Specificare il dispositivo da usare per il nodo, il nodo sul quale sarà applicata questa istanza, il nome del metodo e qualsiasi opzione per questo metodo specifica al nodo:

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

   Per configurare una istanza di fencing nel file di configurazione sul nodo **node-01.example.com** del cluster il quale utilizza la porta 1 dell'interruttore APC sul dispositivo chiamato **apc** per isolare il nodo **node-01.example.com** usando il metodo **APC**, eseguire il seguente comando:

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

3. Aggiungere un metodo di fencing di backup per il nodo fornendone il nome.

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

   Per configurare un metodo di fencing di backup chiamato **SAN** per il nodo **node-01.example.com** nel file di configurazione del nodo **node-01.example.com** eseguire il seguente comando:

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

4. Aggiungere una istanza di fencing per il metodo di backup. Specificare il dispositivo da usare per il nodo, il nodo sul quale sarà applicata questa istanza, il nodo del metodo e le opzioni specifiche a questo nodo:

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

   Per configurare una istanza di fencing nel file di configurazione sul nodo **node-01.example.com** del cluster il quale utilizza la porta 11 dell'interruttore SAN sul dispositivo chiamato **sanswitch1** per isolare il nodo **node-01.example.com** usando il metodo **SAN**, eseguire il seguente comando:

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

5. Poichè il dispositivo **sanswitch1** è un dispositivo basato sullo storage sarà necessario configurare unfencing per questo dispositivo.

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

Continuare ad aggiungere i metodi di fencing in base alle vostre necessità.

Questa procedura configura un dispositivo di fencing ed un dispositivo di backup per un nodo all'interno del cluster. Sarà necessario configurare anche il processo di fencing per altri nodi nel cluster.

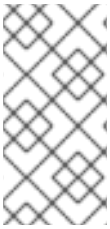
Esempio 5.4, «**cluster.conf** dopo l'aggiunta dei metodi di fencing di backup» mostra un file di configurazione **cluster.conf** dopo aver aggiunto un metodo di fencing primario basato sull'alimentazione ed un metodo di fencing di backup basato sullo storage per ogni nodo nel cluster.

Esempio 5.4. cluster.conf dopo l'aggiunta dei metodi di fencing di backup

```
<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>
```

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».



NOTA

L'ordine con il quale il sistema utilizza i metodi di fencing configurati segue l'ordine riportato nel file di configurazione del cluster. Il primo metodo configurato è il metodo primario, il secondo metodo sarà quello di backup. Per modificare l'ordine rimuovere il metodo primario dal file di configurazione per poi aggiungerlo nuovamente.

5.7.4. Configurazione di un nodo con alimentazione ridondante

Se il cluster è stato configurato con sorgenti di alimentazione ridondanti sarà necessario configurare un processo di fencing in modo da arrestare completamente i nodi interessati prima di essere isolati. Se configurate ogni sorgente di alimentazione come metodo di fencing separato, ogni sorgente di alimentazione sarà isolato separatamente; il secondo sorgente permetterà al sistema di continuare l'esecuzione quando il primo sorgente risulta isolato, così facendo il sistema non sarà isolato. Per configurare un sistema con sorgente di alimentazione doppia configurare i dispositivi di fencing in modo tale che entrambi i sorgenti di alimentazione siano arrestati ed il sistema completamente disattivato. Per fare questo sarà necessario configurare due istanze all'interno di un metodo di fencing singolo, e per ogni istanza sarà necessario configurare entrambi i dispositivi di fencing con un attributo **`action`** su **`off`** prima di configurare ogni dispositivo con un attributo **`action`** su **`on`**.

Per configurare un processo di isolamento per un nodo con sorgente di alimentazione doppia seguire le fasi riportate in questa sezione.

1. Prima di configurare il fencing per un nodo con alimentazione ridondante sarà necessario configurare ogni interruttore di alimentazione come un dispositivo di fencing per il cluster. Per informazioni su come configurare i dispositivi di fencing consultare Sezione 5.5, «Configurazione dei dispositivi di fencing».

   Per stampare un elenco di dispositivi di fencing disponibili per il cluster eseguire il seguente comando:

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

2. Aggiungere un metodo di fencing per il nodo e specificare un nome.

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

   Per esempio per configurare un metodo chiamato **`APC-dual`** per il nodo **`node-01.example.com`** nel file di configurazione sul nodo del cluster **`node-01.example.com`**, eseguire il seguente comando:

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

3. Per il primo sorgente di alimentazione aggiungere una istanza al metodo di fencing. Specificare il dispositivo di fencing da usare per il nodo, il nodo al quale viene applicata questa istanza, il nome del metodo e qualsiasi opzione per questo metodo specifica al nodo. A questo punto configurare l'attributo **action** su **off**.

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

Per configurare una istanza di fencing nel file di configurazione sul nodo **node-01.example.com** del cluster il quale utilizza la porta 1 dell'interruttore APC sul dispositivo chiamato **apc1** per isolare il nodo **node-01.example.com** usando il metodo **APC-dual** ed impostare l'attributo **action** su **off**, eseguire il seguente comando:

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

4. Per il secondo sorgente di alimentazione aggiungere una istanza al metodo di fencing. Specificare il dispositivo di fencing da usare per il nodo, il nodo al quale viene applicata questa istanza, il nome del metodo e qualsiasi opzione per questo metodo specifica al nodo. A questo punto configurare l'attributo **action** su **off**.

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

Per esempio per configurare una seconda istanza per il fencing nel file di configurazione sul nodo **node-01.example.com** del cluster, il quale utilizza la porta 1 dell'interruttore APC sul dispositivo chiamato **apc2** per isolare il nodo **node-01.example.com** usando lo stesso metodo specificato per la prima istanza, **APC-dual**, ed impostare l'attributo **action** su **off**, eseguire il seguente comando:

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

5. A questo punto aggiungere un'altra istanza al metodo di fencing per il primo sorgente di alimentazione configurando l'attributo **action** su **on**. Specificare il dispositivo di fencing da usare per il nodo, il nodo sul quale viene applicata questa istanza, il nome del metodo e qualsiasi opzione per questo metodo specifica al nodo, e specificare l'attributo **action** su **on**:

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

Per configurare una istanza di fencing nel file di configurazione sul nodo **node-01.example.com** del cluster il quale utilizza la porta 1 dell'interruttore APC sul dispositivo chiamato **apc1** per isolare il nodo **node-01.example.com** usando il metodo **APC-dual** ed impostare l'attributo **action** su **on**, eseguire il seguente comando:

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

6. A questo punto aggiungere un'altra istanza al metodo di fencing per il secondo sorgente di alimentazione specificando l'attributo **action** su **on** per questa istanza. Specificare il dispositivo di fencing da usare per il nodo, il nodo sul quale viene applicata questa istanza, il nome del

metodo e qualsiasi opzione per questo metodo specifica al nodo, e specificare l'attributo **action** su **on**:

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

Per esempio per configurare una seconda istanza per il fencing nel file di configurazione sul nodo **node-01.example.com** del cluster, il quale utilizza la porta 1 dell'interruttore APC sul dispositivo chiamato **apc2** per isolare il nodo **node-01.example.com** usando lo stesso metodo specificato per la prima istanza, **APC-dual**, ed impostare l'attributo **action** su **on**, eseguire il seguente comando:

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

Esempio 5.5, «**cluster.conf** dopo aver aggiunto un Dual-Power Fencing» mostra un file di configurazione **cluster.conf** dopo aver aggiunto il fencing per due sorgenti di alimentazione per ogni node nel cluster.

Esempio 5.5. cluster.conf dopo aver aggiunto un Dual-Power Fencing

```
<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>
```

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.7.5. Rimozione dei metodi e delle istanze del fencing

Per rimuovere un metodo di fencing dalla configurazione del cluster eseguire il seguente comando:

```
ccs -h host --rmmethod method node
```

Per esempio, per rimuovere un metodo chiamato **APC** configurato per **node01.example.com** dal file di configurazione del cluster sul nodo **node01.example.com**, eseguire il seguente comando:

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

Per rimuovere tutte le istanze di un dispositivo da un metodo di fencing eseguire il seguente comando:

```
ccs -h host --rmfenceinst fencedevicename node method
```

Per esempio, per rimuovere tutte le istanze dal dispositivo **apc1** dal metodo **APC-dual** configurato per **node01.example.com** dal file di configurazione del cluster sul nodo **node01.example.com**, eseguire il seguente comando:

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

5.8. CONFIGURAZIONE DI UN DOMINIO DI FAILOVER

Un dominio di failover è un sottoinsieme di nodi del cluster idonei alla esecuzione di un servizio in presenza di un errore del nodo. Un dominio di failover può avere le seguenti caratteristiche:

- Unrestricted — Permette di specificare un insieme di membri preferiti, ed un servizio assegnato a questo dominio può essere eseguito su qualsiasi membro disponibile.
- Restricted — Permette di limitare i membri sui quali un servizio può essere eseguito. Se nessun membro presente in un dominio di failover limitato è disponibile, il servizio non potrà essere avviato (sia manualmente che dal software del cluster).

- Unordered — Quando un servizio viene assegnato a questo tipo di dominio di failover il membro sul quale viene eseguito il servizio viene selezionato dai membri disponibili del dominio senza seguire alcuna priorità.
- Ordered — Permette di specificare un ordine preferito dei membri di un dominio. Il primo membro dell'elenco è quello preferito, seguito dal secondo e così via.
- Failback — Permette di specificare se un servizio in un dominio di failover può essere eseguito sul nodo sul quale era in esecuzione prima del fallimento del nodo stesso. La configurazione di questa caratteristica è utile in situazioni dove un nodo fallisce ripetutamente ed è parte di un dominio ordinato (ordered). In tale situazione, se un nodo è quello preferito in un dominio di failover, sarà possibile eseguire il failover ed il failback del servizio tra il nodo preferito ed un altro nodo, causando un impatto negativo severo sulle prestazioni.

NOTA

La caratteristica di failback è applicabile solo se è stato configurato un dominio di failover ordinato.

NOTA

La modifica della configurazione di un dominio di failover non ha alcun effetto sui servizi attualmente in esecuzione.

NOTA

I domini di failover *non* sono necessari per il funzionmento.

Per impostazione predefinita i domini di failover sono unrestricted e unordered.

In un cluster con diversi membri l'uso di un dominio di failover limitato può minimizzare il lavoro di impostazione del cluster per l'esecuzione di un servizio (come ad esempio **`httpd`**), il quale necessita di una impostazione di una configurazione identica su tutti i membri che eseguono il servizio. Invece di impostare l'intero cluster per l'esecuzione del servizio sarà possibile impostare solo i membri nel dominio di failover limitato 'restricted' associato con il servizio del cluster.

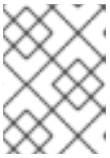
NOTA

Per configurare un membro preferito creare un dominio di failover unrestricted con un solo membro. Così facendo il servizio del cluster verrà eseguito principalmente sul membro in questione (il membro preferito), permettendo il failover del servizio su qualsiasi altro membro.

Per configurare un dominio di failover eseguire la seguente procedura:

1. Per aggiungere il dominio di failover eseguire il seguente comando:

```
ccs -h host --addfailoverdomain name [restricted] [ordered]
[nofailback]
```



NOTA

Il nome dovrebbe essere sufficientemente descrittivo per distinguere i compiti rispetto ad altri nomi usati nel cluster.

Per esempio, il seguente comando configura un dominio di failover chiamato **example_pri** su **node-01.example.com** il quale è 'unrestricted', ordinato e permette un failback:

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

2. Per aggiungere un nodo al dominio di failover eseguire il seguente comando:

```
ccs -h host --addfailoverdomainnode failoverdomain node priority
```

Per esempio, per configurare il dominio di failover **example_pri** nel file di configurazione su **node-01.example.com** in modo da avere **node-01.example.com** con una priorità 1, **node-02.example.com** con priorità 2, e **node-03.example.com** con priorità 3, eseguire i seguenti comandi:

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

Con il seguente comando sarà possibile elencare tutti i domini ed i nodi dei domini di failover configurati in un cluster:

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

Per rimuovere un dominio di failover eseguire il seguente comando:

```
ccs -h host --rmfailoverdomain name
```

Per rimuovere un nodo dal dominio di failover eseguire il seguente comando:

```
ccs -h host --rmfailoverdomainnode failoverdomain node
```

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.9. CONFIGURAZIONE DELLE RISORSE GLOBALI DEL CLUSTER

È possibile configurare due tipi di risorse:

- Globale — Risorse disponibili ad ogni servizio del cluster.
- Servizio-specifico — Risorse disponibili solo ad un servizio.

Per visualizzare un elenco di servizi e risorse configurate nel cluster eseguire il seguente comando:

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

Per aggiungere una risorsa globale del cluster eseguire il seguente comando. Sarà possibile aggiungere una risorsa locale ad un servizio particolare durante la configurazione del servizio come descritto in Sezione 5.10, «Come aggiungere un servizio al cluster».

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

Per esempio, il seguente comando aggiunge una risorsa globale del file system al file di configurazione del cluster su **node01.example.com**. Il nome della risorsa è **web_fs**, il dispositivo del file system è **/dev/sdd2**, il mountpoint è **/var/www**, ed il tipo è **ext3**.

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

Per informazioni sui tipi di risorse disponibili e le rispettive opzioni consultare Appendice B, *Parametri della risorsa HA*.

Per rimuovere una risorsa globale eseguire il seguente comando:

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

Se sarà necessario modificare i parametri di una risorsa globale esistente rimuovere la risorsa e configurarla nuovamente.

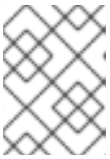
Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.10. COME AGGIUNGERE UN SERVIZIO AL CLUSTER

Per configurare un servizio in un cluster eseguire le seguenti fasi:

1. Aggiungere un servizio al cluster con il seguente comando:

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

   NOTA

   Usare un nome descrittivo il quale distingue in modo chiaro il servizio da altri servizi presenti nel cluster:

   Durante l'aggiunta del servizio alla configurazione del cluster configurare i seguenti attributi

   - **autostart** — Specifica se eseguire un avvio automatizzato del servizio all'avvio del cluster. Usare '1' per abilitare e '0' per disabilitare; l'impostazione predefinita è abilitato.
   - **domain** — Specifica un dominio di failover (se necessario).
   - **exclusive** — Specifica una politica in cui il servizio viene eseguito solo su nodi sprovvisti di altri servizi.

- **recovery** — Specifica una politica di ripristino per il servizio. Le opzioni possibili sono relocate, restart, disable, o restart-disable. Selezionando Restart il sistema cercherà di riavviare il servizio fallito prima di riposizionare il servizio stesso su un altro nodo. Con Relocate il sistema dovrà riavviare il servizio su un nodo diverso. Selezionando l'opzione Disable verrà indicato al sistema di disabilitare il gruppo di risorse se qualsiasi componente fallisce. Restart-Disable indica al sistema di riavviare il servizio fallito ma se il riavvio fallisce il servizio sarà disabilitato e non sarà riposizionato sugli host del cluster.

  Se selezionate **Restart** o **Restart-Disable** come politica di ripristino del servizio, sarà possibile specificare il numero massimo di fallimenti prima di eseguire il riposizionamento o disabilitare il servizio, e l'arco di tempo, espresso in secondi, dopo il quale non eseguire più alcun processo di riavvio.

Per esempio, per aggiungere un servizio al file di configurazione sul nodo **node-01.example.com** chiamato **example_apache** il quale utilizza un dominio di failover **example_pri**, con una politica di ripristino **relocate**, eseguire il seguente comando:

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

Durante la configurazione dei servizi di un cluster è consigliato consultare l'elenco dei servizi disponibili e delle opzioni presenti per ogni servizio. Per informazioni aggiuntive su come utilizzare il comando **ccs** per stampare un elenco di dispositivi di fencing disponibili, opzioni o un elenco di servizi e delle opzioni correlate consultare Sezione 5.11, «Elenco dei servizi cluster disponibili».

2. Aggiungere le risorse al servizio con il seguente comando:

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

In base al tipo di risorse che desiderate aggiungere popolare il servizio con risorse globali o specifiche al servizio. Per aggiungere una risorsa globale usare l'opzione **--addsubservice** del **ccs**. Per esempio, per aggiungere la risorsa globale del file system chiamata **web_fs** al servizio **example_apache** del file di configurazione del cluster su **node-01.example.com**, eseguire il seguente comando:

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

Per aggiungere una risorsa specifica al servizio sarà necessario specificare tutte le opzioni del servizio. Se non avete precedentemente definito **web_fs** come servizio globale sarà possibile aggiungerlo come risorsa specifica al servizio con il seguente comando:

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

3. Per aggiungere un servizio figlio è possibile usare anche l'opzione **--addsubservice** del comando **ccs** specificando le opzioni del servizio.

Se desiderate aggiungere i servzi all'interno di una struttura dell'albero delle dipendenze usare il carattere (":") per separare gli elementi, e le parentesi per identificare i servizi secondari dello stesso tipo. Il seguente esempio aggiunge un terzo servizio **nfsclient** come servizio secondario di **nfsclient** il quale rappresenta un servizio secondario di un **nfsclient** che a sua volta è un servizio secondario di **service_a**:

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

NOTA

Se desiderate aggiungere una risora servizio-Samba aggiungetela direttamente al servizio ma *non* come figlio di un'altra risorsa.

NOTA

Per verificare l'esistenza della risorsa del servizio IP usata in un servizio del cluster, usare il comando **/sbin/ip addr show** su un nodo del cluster (al posto del comando **ifconfig**). Il seguente output mostra il comando **/sbin/ip addr show** eseguito su un nodo che esegue il servizio del cluster:

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

Per rimuovere un servizio insieme a tutti i suoi servizi secondari eseguire il seguente comando:

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

Per rimuovere un servizio secondario eseguire il seguente comando:

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

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.11. ELENCO DEI SERVIZI CLUSTER DISPONIBILI

Usare il comando **ccs** per stampare un elenco di servizi disponibili per il cluster. È possibile altresì usare il comando **ccs** per un elenco di opzioni utilizzabili per un tipo di servizio particolare.

Per stampare un elenco di servizi disponibili per il cluster eseguire il seguente comando:

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

Il seguente comando elenca i servizi disponibili sul nodo del cluster **node1**, e mostra un output d'esempio.

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

Per stampare un elenco di opzioni da specificare per un tipo di servizio usare il seguente comando:

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

Il seguente comando elenca le opzioni del servizio per **vm**.

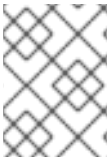
```
[root@ask-03 ~]# ccs -f node1 --lsserviceopts vm
vm - Defines a Virtual Machine
  Required Options:
    name: Name
  Optional Options:
    domain: Cluster failover Domain
    autostart: Automatic start after quorum formation
    exclusive: Exclusive resource group
    recovery: Failure recovery policy
    migration_mapping: memberhost:targethost,memberhost:targethost ..
    use_virsh: If set to 1, vm.sh will use the virsh command to manage
virtual machines instead of xm. This is required when using non-Xen
virtual machines (e.g. qemu / KVM).
    xmlfile: Full path to libvirt XML file describing the domain.
    migrate: Migration type (live or pause, default = live).
    path: Path to virtual machine configuration files.
    snapshot: Path to the snapshot directory where the virtual machine
image will be stored.
    depend: Top-level service this depends on, in service:name format.
    depend_mode: Service dependency mode (soft or hard).
    max_restarts: Maximum restarts for this service.
    restart_expire_time: Restart expiration time; amount of time before a
```

```
restart is forgotten.
    status_program: Additional status check program
    hypervisor: Hypervisor
    hypervisor_uri: Hypervisor URI (normally automatic).
    migration_uri: Migration URI (normally automatic).
    __independent_subtree: Treat this and all children as an independent
subtree.
    __enforce_timeouts: Consider a timeout for operations as fatal.
    __max_failures: Maximum number of failures before returning a failure
to a status check.
    __failure_expire_time: Amount of time before a failure is forgotten.
    __max_restarts: Maximum number restarts for an independent subtree
before giving up.
    __restart_expire_time: Amount of time before a failure is forgotten
for an independent subtree.
```

5.12. RISORSE DELLA MACCHINA VIRTUALE

Le risorse della macchina virtuale sono configurate in modo diverso da altre risorse del cluster. In particolare esse non sono raggruppate in definizioni del servizio. Con Red Hat Enterprise Linux 6.2 durante la configurazione di una macchina virtuale in un cluster con il comando **ccs**, è possibile utilizzare **--addvm** (al posto dell'opzione **addservice**). Così facendo la risorsa **vm** verrà definita direttamente con il nodo di configurazione **rm** nel file di configurazione del cluster.

Come requisiti minimi una risorsa della macchina virtuale ha bisogno di un attributo **name** e **path**. L'attributo **name** deve corrispondere al nome del dominio **libvirt** mentre **path** deve specificare la directory dove sono archiviate le definizioni della macchina virtuale condivisa.



NOTA

L'attributo **path** in un file di configurazione del cluster rappresenta il percorso o un nome della directory e non un percorso per un singolo file.

Se le definizioni della macchina virtuale sono archiviate in una directory **/mnt/vm_defs** condivisa, il seguente comando definirà una macchina virtuale chiamata **guest1**:

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

L'esecuzione di questo comando aggiungerà la seguente riga al nodo di configurazione **rm** nel file **cluster.conf**:

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

5.13. CONFIGURAZIONE DI UN QUORUM DISK

NOTA

I valori euristici ed i parametri del Quorum-disk dipendono dall'ambiente del sito e dai requisiti speciali. Per comprendere l'uso degli euristici e dei parametri del quorum-disk consultare la pagina man qdisk(5). Se avete bisogno di assistenza per l'utilizzo e la comprensione del quorum disk contattate un rappresentante autorizzato per il supporto di Red Hat.

Usare il seguente comando per configurare il sistema all'uso di un quorum disk:

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

Da notare che questo comando resetta tutte le proprietà da impostare con il comando **`--setquorumd`**, sui rispettivi valori predefiniti come descritto in Sezione 5.1.5, «Comandi che sovrascrivono le impostazioni precedenti».

Tabella 5.1, «Opzioni del quorum disk» riassume il significato delle opzioni del quorum disk da impostare. Per un elenco completo di parametri del quorum disk consultare gli schemi riportati su **`/usr/share/cluster/cluster.rng`** e **`/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html`**.

Tabella 5.1. Opzioni del quorum disk

Parametro	Descrizione
interval	La frequenza dei cicli di lettura/scrittura in secondi.
votes	Il numero di voti resi noti dal demone del quorum al comando **`cman`** in presenza di un punteggio sufficientemente alto.
tko	Il numero di cicli persi da un nodo prima di essere dichiarato morto.
min_score	Il punteggio minimo per considerare un nodo 'vivo' "alive". Se omesso o impostato su 0, la funzione predefinita, verrà utilizzato **`floor((`*`n`*`+1)/2)`**, dove *n* rappresenta la somma dei punteggi euristici. Il valore **Minimum Score** non deve eccedere mai la somma dei punteggi euristici; in caso contrario il quorum disk non sarà disponibile.
device	Il dispositivo di storage usato dal quorum disk. Il dispositivo deve essere uguale su tutti i nodi.
label	Specifica l'etichetta del quorum disk creata da **`mkqdisk`**. Se questo campo contiene una voce l'etichetta sovrascrive il campo **Device**. Se utilizzate questo campo il demone del quorum leggerà **`/proc/partitions`** e controllerà la presenza delle firme su ogni dispositivo a blocchi trovato, confrontando l'etichetta con quella specificata. Tale impostazione è utile in configurazioni dove il nome del dispositivo quorum presente nei nodi non è uguale.

Utilizzare il seguente comando per configurare gli euristici per un quorum disk:

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

Tabella 5.2, «Euristici del Quorum Disk» riassume il significato degli euristici del quorum disk da impostare.

Tabella 5.2. Euristici del Quorum Disk

Parametro	Descrizione
program	Il Percorso per il programma usato per determinare se questo valore euristico è disponibile. Può essere un valore qualsiasi eseguibile da **`/bin/sh -c`**. Un valore indica un successo; qualsiasi altra cosa indica un errore. Questo parametro è obbligatorio per poter usare un disco quorum.
interval	La frequenza (in secondi) con la quale viene verificato l'euristico. L'intervallo predefinito per ogni euristico è 2 secondi.
score	Il peso di questo euristico. Fare attenzione durante la determinazione dei risultati per gli euristici. Il risultato predefinito per ogni euristico è 1.
tko	Il numero di fallimenti consecutivi prima di poter dichiarare questo euristico non disponibile.

Per visualizzare un elenco di opzioni del quorum disk e degli euristici configurati su un sistema eseguire il seguente comando:

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

Per rimuovere un euristico specificato da una opzione eseguire il seguente comando:

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

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

NOTA

La sincronizzazione e l'attivazione propagano ed attivano il file di configurazione aggiornato. Tuttavia per un funzionamento corretto del quorum disk riavviare il cluster (consultate Sezione 6.2, «Avvio ed arresto di un cluster»), ed assicurarsi di aver riavviato il demone **`qdiskd`** su ogni nodo.

5.14. CONFIGURAZIONI VARIE DEL CLUSTER

Questa sezione descrive l'utilizzo del comando **`ccs`** per configurare quanto di seguito riportato:

- Sezione 5.14.1, «Versione della configurazione del cluster»
- Sezione 5.14.2, «Configurazione Multicast»
- Sezione 5.14.3, «Configurazione di un cluster a due nodi»
- Sezione 5.14.4, «Registrazione»

- Sezione 5.14.5, «Configurazione Protocollo ring ridondante»

È possibile usare il comando **ccs** per impostare i parametri avanzati di configurazione del cluster, incluse le opzioni **totem**, **dlm**, **rm** e **cman**. Per informazioni su come impostare questi parametri consultare la pagina man **ccs**(8) e lo schema del file di configurazione del cluster presente su **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Per visualizzare un elenco di attributi vari del cluster configurati eseguire il seguente comando:

```
ccs -h host --lsmisc
```

5.14.1. Versione della configurazione del cluster

Un file di configurazione contiene un valore relativo alla versione della configurazione del cluster. Questo valore è impostato su **1** per impostazione predefinita durante la creazione di un file di configurazione del cluster, e viene automaticamente aumentato ad ogni modifica della configurazione. Per impostarlo su un altro valore, specificatelo con il seguente comando:

```
ccs -h host --setversion n
```

Per ottenere il valore della versione corrente su di un file di configurazione del cluster usare il seguente comando:

```
ccs -h host --getversion
```

Per aumentare il valore della versione di una (1) unità su ogni nodo del cluster eseguire il seguente comando:

```
ccs -h host --incversion
```

5.14.2. Configurazione Multicast

Se non specificate un indirizzo multicast nel file di configurazione del cluster il software Red Hat High Availability Add-On ne creerà uno in base all'ID del cluster. Così facendo verranno generati i 16 bit più bassi dell'indirizzo i quali verranno aggiunti alla sezione più alta dell'indirizzo in base al tipo di protocollo IP, IPV4 o IPV6:

- Per IPV4 — L'indirizzo formato è 239.192. più i 16 bit più bassi generati dal software Red Hat High Availability Add-On.
- Per IPV6 — L'indirizzo formato è FF15:: più i 16 bit più bassi generati dal software Red Hat High Availability Add-On.

NOTA

L'ID del cluster è un identificatore unico generato da **cman** per ogni cluster. Per poter visualizzare il suddetto ID eseguire **cman_tool status** sul nodo.

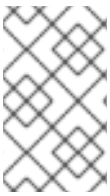
È possibile specificare un indirizzo multicast nel file di configurazione con il seguente comando:

```
ccs -h host --setmulticast multicastaddress
```

Da notare che questo comando resetta tutte le proprietà da impostare con **--setmulticast** sui rispettivi valori predefiniti come descritto in Sezione 5.1.5, «Comandi che sovrascrivono le impostazioni precedenti».

Se specificate un indirizzo multicast usare la serie 239.192.x.x (o FF15:: per IPv6) usata da **cman**. In caso contrario l'uso esterno dell'indirizzo multicast dalla gamma specificata potrebbe causare risultati imprevedibili. Per esempio se utilizzate 224.0.0.x ("Tutti gli host sulla rete") si potrebbe verificare un instradamento non corretto oppure, con alcuni tipi di hardware, l'instradamento potrebbe non verificarsi.

Se specificate o modificate un indirizzo multicast sarà necessario riavviare il cluster per implementare le modifiche. Per informazioni su come avviare o arrestare un cluster con **ccs** consultare Sezione 6.2, «Avvio ed arresto di un cluster».



NOTA

Se specificate un indirizzo multicast assicuratevi di controllare la configurazione dei router utilizzati dai pacchetti del cluster. Alcuni router potrebbero impiegare un tempo molto lungo per accettare gli indirizzi impattando così negativamente sulle prestazioni.

Per rimuovere un indirizzo multicast da un file di configurazione usare l'opzione **--setmulticast** di **ccs** senza specificare alcun indirizzo multicast:

```
ccs -h host --setmulticast
```

5.14.3. Configurazione di un cluster a due nodi

Se configurate un cluster a due nodi eseguire il seguente comando in modo da permettere il mantenimento del quorum da parte di un singolo nodo (per esempio in caso di fallimento di un nodo):

```
ccs -h host --setcman two_node=1 expected_votes=1
```

Da notare che questo comando resetta tutte le proprietà da impostare con **--setcman** sui rispettivi valori predefiniti come descritto in Sezione 5.1.5, «Comandi che sovrascrivono le impostazioni precedenti».

Utilizzando il comando **ccs --setcman** per aggiungere, rimuovere o modificare l'opzione **two_node** sarà necessario riavviare il cluster per implementare le modifiche. Per informazioni su come avviare o arrestare un cluster con **ccs** consultare Sezione 6.2, «Avvio ed arresto di un cluster».

5.14.4. Registrazione

È possibile abilitare il debugging per tutti i demoni in un cluster oppure la registrazione per processazioni del cluster specifiche.

Per abilitare il debugging per tutti i demoni eseguire il seguente comando. Per impostazione predefinita la registrazione viene eseguita su **/var/log/cluster/*daemon*.log**.

```
ccs -h host --setlogging [logging options]
```

Per esempio, il seguente comando abilita il debugging per tutti i demoni.

```
# ccs -h node1.example.com --setlogging debug=on
```

Da notare che questo comando resetta tutte le proprietà da impostare con **--setlogging** sui rispettivi valori predefiniti come descritto in Sezione 5.1.5, «Comandi che sovrascrivono le impostazioni precedenti».

Per abilitare il debugging per processi individuali del cluster eseguire il seguente comando. La configurazione della registrazione per-demone sovrascrive le impostazioni globali.

```
ccs -h host --addlogging [logging daemon options]
```

I seguenti comandi abilitando il debugging per i demoni **corosync** e **fenced**.

```
# ccs -h node1.example.com --addlogging name=corosync debug=on
# ccs -h node1.example.com --addlogging name=fenced debug=on
```

Per rimuovere le impostazioni per i singoli demoni usare il seguente comando.

```
ccs -h host --rmlogging name=clusterprocess
```

Per esempio, il seguente comando rimuove le impostazioni del log specifiche al demone per il demone **fenced**

```
ccs -h host --rmlogging name=fenced
```

Per un elenco dei demoni per i quali è possibile abilitare la registrazione insieme alle opzioni aggiuntive per una registrazione per-demone e globale, consultare la pagina man di **cluster.conf**(5).

Dopo aver terminato la configurazione di tutti i componenti del cluster sarà necessario sincronizzare il file di configurazione con tutti i nodi come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.14.5. Configurazione Protocollo ring ridondante

Con Red Hat Enterprise Linux 6.4, Red Hat High Availability Add-On rende disponibile il supporto per la configurazione del protocollo ring ridondante. Durante l'uso del suddetto protocollo è consigliato considerare un certo numero di fattori come riportato in Sezione 7.6, «Configurazione Protocollo ring ridondante».

Per specificare una seconda interfaccia di rete per l'utilizzo di un protocollo ring ridondante, aggiungere un nome alternativo per il nodo usando l'opzione **--addalt** del comando **ccs**:

```
ccs -h host --addalt node_name alt_name
```

Per esempio il seguente comando configura il nome alternativo **clusternet-node1-eth2** per il nodo **clusternet-node1-eth1**:

```
# ccs -h clusternet-node1-eth1 --addalt clusternet-node1-eth1 clusternet-
node1-eth2
```

Se necessario specificare manualmente un indirizzo multicast, una porta ed un TTL per il secondo ring. Se specificate un indirizzo multicast per il secondo ring, l'indirizzo o la porta alternativi devono essere diversi dall'indirizzo multicast per il primo ring. Se specificate una porta alternativa i numeri della porta

del primo ring e del secondo ring devono differire di almeno due unità poichè il sistema utilizza un valore porta e porta-1 per eseguire le operazioni necessarie. Se non specificate alcun indirizzo alternativo per il secondo ring, il sistema userà automaticamente un indirizzo multicast diverso.

Per specificare un indirizzo multicast, una porta, o un TTL alternativi per il secondo ring usare l'opzione **--setaltmulticast** del comando **ccs**:

```
ccs -h host --setaltmulticast [alt_multicast_address]
[alt_multicast_options].
```

Per esempio, il seguente comando imposta un indirizzo multicast alternativo 239.192.99.88, una porta 888, ed un TTL di 3 per il cluster definito nel file **cluster.conf** sul nodo **clusternet-node1-eth1**:

```
ccs -h clusternet-node1-eth1 --setaltmulticast 239.192.99.88 port=888
ttl=3
```

Per rimuovere un indirizzo multicast specificare l'opzione **--setaltmulticast** del comando **ccs** senza specificare un indirizzo multicast. Da notare che questo comando resetta tutte le proprietà da impostare con il comando **--setaltmulticast** sui rispettivi valori predefiniti come descritto in Sezione 5.1.5, «Comandi che sovrascrivono le impostazioni precedenti».

Una volta terminata la configurazione di tutti i componenti del cluster sarà necessario eseguire la sincronizzazione del file di configurazione del cluster su tutti i nodi come riportato in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

5.15. PROPAGAZIONE DEL FILE DI CONFIGURAZIONE AI NODI DEL CLUSTER

Dopo aver creato o modificato un file di configurazione del cluster su uno dei nodi sarà necessario propagare lo stesso file su tutti i nodi del cluster ed attivare la configurazione.

Usare il seguente comando per propagare ed attivare un file di configurazione del cluster:

```
ccs -h host --sync --activate
```

Per verificare che tutti i nodi specificati nel file di configurazione del cluster host sono in possesso di un file di configurazione identico eseguire il seguente comando:

```
ccs -h host --checkconf
```

Se avete creato o modificato un file di configurazione su un nodo locale usare il seguente comando per inviare il file in questione ad uno dei nodi del cluster:

```
ccs -f file -h host --setconf
```

Per verificare che tutti i nodi specificati nel file locale siano in possesso di un file di configurazione identico eseguire il seguente comando:

```
ccs -f file --checkconf
```

CAPITOLO 6. GESTIONE DI RED HAT HIGH AVAILABILITY ADD-ON CON CCS

Questo capitolo descrive i vari compiti amministrativi per la gestione di Red Hat High Availability Add-On attraverso il comando **ccs** supportato con la release Red Hat Enterprise Linux 6.1 e versioni più recenti. Questo capitolo consiste nelle seguenti sezioni:

- Sezione 6.1, «Gestione dei nodi del cluster»
- Sezione 6.2, «Avvio ed arresto di un cluster»
- Sezione 6.3, «Diagnosi e correzione dei problemi presenti nel cluster»

6.1. GESTIONE DEI NODI DEL CLUSTER

Questa sezione indica come eseguire le funzioni di gestione dei nodi con il comando **ccs**:

- Sezione 6.1.1, «Esclusione o inserimento di un nodo nel cluster»
- Sezione 6.1.2, «Come aggiungere un membro ad un cluster in esecuzione»

6.1.1. Esclusione o inserimento di un nodo nel cluster

È possibile usare il comando **ccs** per causare l'uscita dal cluster da parte di un nodo arrestando i servizi del cluster sul nodo in questione. L'abbandono del cluster non rimuoverà le informazioni sulla configurazione del cluster presenti sul nodo. Questa operazione impedisce al nodo di unirsi automaticamente al cluster se riavviato.

Per rimuovere un nodo dal cluster eseguire il seguente comando il quale arresta i servizi del cluster sul nodo specificato con l'opzione **-h**:

```
ccs -h host --stop
```

Quando arrestate i servizi del cluster su un nodo, i servizi in esecuzione verranno passati su un altro nodo (failover).

Per rimuovere completamente un nodo dalla configurazione del cluster usare l'opzione **--rmnode** del comando **ccs** come riportato in Sezione 5.4, «Creazione di un cluster».

Per introdurre nuovamente un nodo nel cluster eseguire il seguente comando in grado di avviare i servizi del cluster sul nodo specificato con l'opzione **-h**:

```
ccs -h host --start
```

6.1.2. Come aggiungere un membro ad un cluster in esecuzione

Per aggiungere un membro in un cluster in esecuzione aggiungere il nodo al cluster come descritto in Sezione 5.4, «Creazione di un cluster». Dopo aver aggiornato il file di configurazione propagare il file su tutti i nodi nel cluster ed attivare il nuovo file di configurazione del cluster come descritto in Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».

6.2. AVVIO ED ARRESTO DI UN CLUSTER

Usare **ccs** per arrestare il cluster. Per fare questo utilizzare il comando per arrestarne i servizi su tutti i nodi:

```
ccs -h host --stopall
```

Usare **ccs** per avviare un cluster non in esecuzione. Per fare questo utilizzare il seguente comando per avviare i servizi su tutti i nodi presenti nel cluster:

```
ccs -h host --startall
```

6.3. DIAGNOSI E CORREZIONE DEI PROBLEMI PRESENTI NEL CLUSTER

Per informazioni sulla diagnosi e correzione dei problemi in un cluster consultare Capitolo 9, *Diagnosi e correzione dei problemi presenti nel cluster*. Tuttavia è possibile eseguire alcuni controlli con il comando **ccs**.

Per verificare che tutti i nodi presenti nel file di configurazione del cluster dell'host siano in possesso di un file di configurazione identico eseguire il seguente comando:

```
ccs -h host --checkconf
```

Se avete creato o modificato un file di configurazione su un nodo locale sarà possibile verificare che tutti i nodi specificati nel file locale siano in possesso di file di configurazione identici tramite il seguente comando:

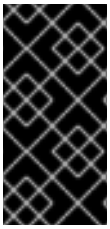
```
ccs -f file --checkconf
```

CAPITOLO 7. CONFIGURAZIONE DI RED HAT HIGH AVAILABILITY ADD-ON CON I TOOL DELLA LINEA DI COMANDO

Questo capitolo descrive il metodo attraverso il quale è possibile configurare il software di Red Hat High Availability Add-On modificando il file di configurazione del cluster (**/etc/cluster/cluster.conf**) ed utilizzando i tool della linea di comando. Il capitolo fornisce le procedure sulla compilazione di un file di configurazione iniziando con un file d'esempio presente nel capitolo. Come alternativa all'uso di un file d'esempio sarà possibile copiare la struttura di un file di configurazione dalla pagina man di **cluster.conf**. Tuttavia così facendo alcune delle informazioni fornite in questo capitolo potrebbero non essere applicabili al vostro contesto. A tale scopo sono a dispositizione altri metodi per la creazione e configurazione di un file di configurazione del cluster; questo capitolo fornisce le procedure necessarie alla compilazione di un file di configurazione. Altresì ricordatevi che questo rappresenta solo un punto di partenza per lo sviluppo di un file di configurazione per soddisfare i vostri requisiti di clustering.

Questo capitolo consiste nelle seguenti sezioni:

- Sezione 7.1, «Fasi necessarie per la configurazione»
- Sezione 7.2, «Creazione di un file di configurazione del cluster di base»
- Sezione 7.3, «Configurazione del fencing»
- Sezione 7.4, «Configurazione dei domini di failover»
- Sezione 7.5, «Configurazione dei servizi HA»
- Sezione 7.7, «Configurazione delle opzioni di debug»
- Sezione 7.6, «Configurazione Protocollo ring ridondante»
- Sezione 7.8, «Verifica di una configurazione»

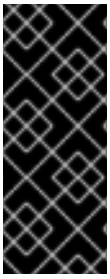


IMPORTANTE

Assicuratevi che l'implementazione High Availability Add-On usata sia supportata e soddisfi i requisiti necessari. Consultate un rappresentante di Red Hat per verificare la configurazione prima di implementarla. Implementate altresì un periodo di prova per le varie modalità d'errore.

IMPORTANTE

Questo capitolo fa riferimento ad attributi ed elementi **cluster.conf** comunemente usati. Per un elenco completo ed una descrizione degli elementi ed attributi di **cluster.conf**, consultate lo schema disponibile su **/usr/share/cluster/cluster.rng**, **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (per esempio **/usr/share/doc/cman-3.0.12/cluster_conf.html**).



IMPORTANTE

Alcune procedure in questo capitolo richiedono l'uso del comando **`cman_tool version -r`** per diffondere la configurazione all'interno di un cluster. L'utilizzo di questo comando richiede l'esecuzione di **`ricci`**. Per usare per la prima volta **ricci** da qualsiasi macchina specifica sarà necessario usare una password. Per informazioni sul servizio **`ricci`** consultare Sezione 2.13, «Considerazioni su **`ricci`**».

NOTA

Le procedure presenti in questo capitolo possono includere comandi specifici per alcuni strumenti della linea di comando elencati in Appendice E, *Sommario dei tool della linea di comando*. Per maggiori informazioni sui comandi e sulle variabili consultare la pagina man di ogni strumento della linea di comando.

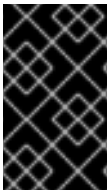
7.1. FASI NECESSARIE PER LA CONFIGURAZIONE

Per configurare Red Hat High Availability Add-On con i tool della linea di comando seguire le fasi di seguito riportate:

1. Creazione di un cluster. Consultare Sezione 7.2, «Creazione di un file di configurazione del cluster di base».
2. Configurazione del fencing. Consultare Sezione 7.3, «Configurazione del fencing».
3. Configurazione dei domini di failover. Consultare Sezione 7.4, «Configurazione dei domini di failover».
4. Configurazione dei servizi HA. Consultare Sezione 7.5, «Configurazione dei servizi HA».
5. Verifica di una configurazione. Consultare Sezione 7.8, «Verifica di una configurazione».

7.2. CREAZIONE DI UN FILE DI CONFIGURAZIONE DEL CLUSTER DI BASE

Previa installazione hardware del cluster, Red Hat Enterprise Linux, e del software High Availability Add-On, sarà possibile creare un file di configurazione del cluster (**`/etc/cluster/cluster.conf`**) ed iniziare l'esecuzione dell'High Availability Add-On. Come punto di partenza questa sezione descrive il metodo attraverso il quale creare la struttura di un file di configurazione del cluster senza fencing, domini di failover e servizi HA. Le sezioni seguenti descrivono il metodo per la configurazione delle varie parti del file di configurazione.



IMPORTANTE

Questa è solo una fase provvisoria per la creazione del file di configurazione del cluster; il file risultante non presenta alcun fencing e non viene considerato come configurazione supportata.

Le fasi di seguito riportate descrivono il metodo attraverso il quale creare e configurare una struttura del file di configurazione del cluster. Il file di configurazione del cluster varia in base al numero dei nodi, tipo di fencing, tipo e numero di servizi HA ed altri requisiti specifici.

1. Su di un nodo del cluster create **/etc/cluster/cluster.conf** utilizzando il template dell'esempio in Esempio 7.1, «**cluster.conf** Esempio: Configurazione di base».

2. **(Opzionale)** Se configurate un cluster con due nodi sarà possibile aggiungere la seguente riga sul file di configurazione, così facendo un singolo nodo sarà in grado di mantenere il quorum (per esempio in caso di fallimento di un nodo):

   <cman two_node="1" expected_votes="1"/>

   Quando aggiungete o rimuovete l'opzione **two_node** dal file **cluster.conf**, sarà necessario riavviare il cluster per poter implementare le modifiche al momento dell'aggiornamento della configurazione. Per informazioni su come aggiornare la configurazione del cluster consultare Sezione 8.4, «Aggiornamento di una configurazione». Per un esempio su come specificare l'opzione **two_node** consultare Esempio 7.2, «**cluster.conf** Esempio: Configurazione di base con due nodi».

3. Specificare la versione della configurazione ed il nome del cluster usando gli attributi **cluster**: **name** e **config_version** (consultare Esempio 7.1, «**cluster.conf** Esempio: Configurazione di base» o Esempio 7.2, «**cluster.conf** Esempio: Configurazione di base con due nodi»).

4. Nella sezione **clusternodes** specificare il nome e l'ID di ogni nodo usando gli attributi **clusternode**: **name** e **nodeid**.

5. Salvare **/etc/cluster/cluster.conf**.

6. Convalidare il file con lo schema del cluster (**cluster.rng**) eseguendo il comando **ccs_config_validate**. Per esempio:

   ```
   [root@example-01 ~]# ccs_config_validate
   Configuration validates
   ```

7. Diffondere il file di configurazione su **/etc/cluster/** in ogni nodo del cluster. Per esempio è possibile diffondere il file su altri nodi del cluster usando il comando **scp**.

   NOTA

   Ciò è necessario durante la creazione del cluster. Dopo l'installazione e l'esecuzione del cluster sarà possibile diffondere il file di configurazione usando **cman_tool version -r**. Per la diffusione di un file di configurazione aggiornato sarà possibile usare il comando **scp**; tuttavia il software del cluster dovrà essere arrestato su tutti i nodi durante l'utilizzo del comando **scp**. In aggiunta eseguire **ccs_config_validate** se diffondete un file di configurazione tramite **scp**.

   NOTA

   Anche se sono presenti elementi ed attributi aggiuntivi in un file di configurazione d'esempio (per esempio **fence** e **fencedevices**) non vi è alcuna necessità di popolarli ora. Le procedure di seguito riportate in questo capitolo forniscono le informazioni relative ad altri elementi ed attributi.

8. Avviare il cluster. Su ogni nodo del cluster eseguire il seguente comando:

service cman start

Per esempio:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK
]
   Global setup...                                         [  OK
]
   Loading kernel modules...                               [  OK
]
   Mounting configfs...                                    [  OK
]
   Starting cman...                                        [  OK
]
   Waiting for quorum...                                   [  OK
]
   Starting fenced...                                      [  OK
]
   Starting dlm_controld...                                [  OK
]
   Starting gfs_controld...                                [  OK
]
   Unfencing self...                                       [  OK
]
   Joining fence domain...                                 [  OK
]
```

9. Su ogni nodo del cluster eseguire **cman_tools nodes** per verificare che i nodi siano membri attivi del cluster (contrassegnati con "M" nella colonna dello stato, "Sts"). Per esempio:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

10. Se il cluester è in esecuzione procedere alla Sezione 7.3, «Configurazione del fencing».

Esempi di configurazione di base

Esempio 7.1, «**cluster.conf** Esempio: Configurazione di base» e Esempio 7.2, «**cluster.conf** Esempio: Configurazione di base con due nodi» (per un cluster a due nodi) ognuno fornisce un esempio di file di configurazione del cluster di base come punto d'inizio. Le procedure di seguito riportate in questo capitolo forniscono le informazioni sulla configurazione dei servizi HA e di fencing.

Esempio 7.1. cluster.conf Esempio: Configurazione di base

```
<cluster name="mycluster" config_version="2">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
```

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

Esempio 7.2. `cluster.conf` Esempio: Configurazione di base con due nodi

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

Valore `consensus` per `totem` in un cluster a due nodi

Durante la creazione di un cluster a due nodi se non desiderate aggiungere nodi supplementari al cluster omettere il valore **`consensus`** nel tag **`totem`** in **`cluster.conf`**, così facendo il valore **`consensus`** sarà calcolato automaticamente. Dopo aver calcolato automaticamente il suddetto valore saranno implementate le seguenti regole:

- Se in presenza di un numero minore o uguale a due nodi, il valore **consensus** risulterà essere (token * 0.2), con un tetto di 2000 msec ed una base di 200 msec.
- Se in presenza di tre o più nodi il valore **consensus** risulterà essere (token + 2000 msec)

Se per la configurazione del timeout di consensus utilizzate l'utilità **cman** in questo modo, e se passate da due a tre nodi, (o più nodi) allora sarà necessario riavviare il cluster poichè il timeout di consensus dovrà essere modificato implementando un valore più grande in base al timeout del token.

Se state configurando un cluster a due nodi e desiderate aggiornare la configurazione in futuro passandola ad un numero maggiore di nodi, allora sarà possibile sovrascrivere il timeout di consensus in modo da non riavviare il cluster all'aumentare dei nodi. Per eseguire questa operazione nel file **cluster.conf** seguite quanto di seguito riportato:

```
<totem token="X" consensus="X + 2000" />
```

Da notare che l'analizzatore della configurazione non calcola automaticamente X + 2000. Usare un valore intero e non una equazione.

Il vantaggio dell'utilizzo di un timeout ottimizzato per cluster a due nodi è che il periodo di tempo generale per il failover viene ridotto poichè consensus non risulta essere una funzione del timeout del token.

Da notare che in **cman** per un autorilevamento in presenza di due nodi, il numero dei nodi fisici è l'elemento più importante rispetto alla presenza della direttiva **two_node=1** nel file **cluster.conf**.

7.3. CONFIGURAZIONE DEL FENCING

La configurazione del fencing consiste nello specificare uno o più dispositivi di fencing in un cluster insieme ad uno o più metodi di fencing per ogni nodo (usando un dispositivo di fencing o dispositivo di fencing specificato).

In base al tipo di dispositivo ed al metodo di fencing necessari per la configurazione, configurare **cluster.conf** nel modo seguente:

1. Nella sezione **fencedevices** specificare ogni dispositivo di fencing usando un elemento **fencedevice** e gli attributi relativi al dispositivo di fencing. Esempio 7.3, «Dispositivo APC di fencing aggiunto al **cluster.conf**» mostra un esempio di un file di configurazione con un dispositivo di fencing APC.

2. Nella sezione **clusternodes** all'interno dell'elemento **fence** di ogni sezione **clusternode**, specificare ogni metodo di fencing del nodo. Specificare il nome del metodo, usando **method**, **name**. Specificare il dispositivo di fencing per ogni metodo, usando **device** ed i relativi attributi, **name** insieme ai parametri specifici del dispositivo di fencing. Esempio 7.4, «Metodi di fencing aggiunti a **cluster.conf**» mostra un esempio di metodo di fencing con un dispositivo per ogni nodo nel cluster.

3. Per metodi di fencing non-power (SAN/storage) alla sezione **clusternodes** aggiungere una sezione **unfence**. Così facendo un nodo isolato non verrà riabilitato fino a quando non verrà eseguito prima il riavvio. Per maggiori informazioni su come riabilitare un nodo consultare la pagina man di **fence_node**(8).

   La sezione **unfence** non contiene le sezioni **method** come la sezione **fence**. Essa contiene i riferimenti diretti **device**, i quali riflettono le sezioni del dispositivo corrispondenti per **fence**, con l'aggiunta dell'azione esplicita (**action**) di "on" o "enable". Lo stesso **fencedevice** viene indicato dalle righe **fence** e **unfence device**, e gli stessi argomenti per-nodo devono essere ripetuti.

Specificando l'attributo **action** su "on" o "enable" permetterete l'abilitazione del nodo dopo il riavvio. Esempio 7.4, «Metodi di fencing aggiunti a **cluster.conf**» e Esempio 7.5, «**cluster.conf**: Metodi di fencing multipli per nodo» includono gli esempi degli attributi e degli elementi **unfence**.

Per maggiori informazioni su **unfence** consultare la pagina man di **fence_node**.

4. Aggiornare l'attributo **config_version** aumentando il proprio valore (per esempio, modificandolo da **config_version="2"** a **config_version="3">**).

5. Salvare **/etc/cluster/cluster.conf**.

6. **(Opzionale)** Convalidare il file aggiornato con lo schema del cluster (**cluster.rng**) eseguendo il comando **ccs_config_validate**. Per esempio:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Eseguire il comando **cman_tool version -r** per diffondere la configurazione al resto dei nodi del cluster. Così facendo verrà eseguita anche una convalida aggiuntiva. Per propagare le informazioni aggiornate sulla configurazione del cluster è necessario che **ricci** sia in esecuzione su ogni nodo del cluster.

8. Verificare che il file di configurazione aggiornato è stato diffuso.

9. Procedere alla Sezione 7.4, «Configurazione dei domini di failover».

Se necessario sarà possibile eseguire configurazioni complesse con metodi di fencing multipli per nodo e con dispositivi multipli per metodo di fencing. Quando si specificano metodi di fencing multipli per nodo se il processo di isolamento fallisce usando il primo metodo, **fenced**, il demone in questione prova il metodo successivo e continua con gli altri metodi fino a trovare quello corretto.

Talvolta per isolare un nodo sarà necessario disabilitare due percorsi I/O o due porte di alimentazione. È possibile eseguire questa operazione specificando due o più dispositivi all'interno di un metodo di fencing. **fenced** esegue l'agente per il processo di fencing solo una volta per ogni riga dispositivo-fencing; per avere un esito positivo tutte le operazioni devono avere successo.

sezione chiamata «Esempi di configurazione per il fencing» mostra le configurazioni più complesse.

Maggiori informazioni sulla configurazione di dispositivi specifici per il fencing sono disponibili sulla pagina man dell'agente dispositivo-fencing (per esempio la pagina man di **fence_apc**). Sarà possibile altresì ottenere maggiori informazioni sui parametri di fencing consultando Appendice A, *Parametri del dispositivo di fencing*, gli agenti per il fencing in **/usr/sbin/**, lo schema del cluster su **/usr/share/cluster/cluster.rng**, e lo schema annotato su **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (per esempio, **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

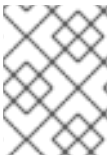
Esempi di configurazione per il fencing

I seguenti esempi riportano una configurazione semplice con un metodo di fencing per nodo ed un dispositivo per metodo di fencing.

- Esempio 7.3, «Dispositivo APC di fencing aggiunto al **cluster.conf**»
- Esempio 7.4, «Metodi di fencing aggiunti a **cluster.conf**»

I seguenti esempi riportano configurazioni piu complesse:

- Esempio 7.5, «**cluster.conf**: Metodi di fencing multipli per nodo»
- Esempio 7.6, «**cluster.conf**: Fencing, Porte multiple Multipath»
- Esempio 7.7, «**cluster.conf**: Nodi per il fencing con gruppo di alimentazione doppio»



NOTA

Gli esempi presenti in questa sezione non sono completi; è possibile configurare il fencing in modo diverso in base ai vostri requisiti.

Esempio 7.3. Dispositivo APC di fencing aggiunto al `cluster.conf`

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

In questo esempio un dispositivo per il fencing (**fencedevice**) è stato aggiunto all'elemento **fencedevices** specificando il fence agent (**agent**) in **fence_apc**, l'indirizzo IP (**ipaddr**) in **apc_ip_example**, il login (**login**) in **login_example**, il nome del dispositivo di fencing (**name**) in **apc**, e la password (**passwd**) in **password_example**.

Esempio 7.4. Metodi di fencing aggiunti a `cluster.conf`

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
```

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

In questo esempio è stato aggiunto un metodo di fencing (**`method`**) ad ogni nodo. Il nome del metodo di fencing (**`name`**) per ogni nodo è **`APC`**. Il dispositivo (**`device`**) per il metodo di fencing in ogni nodo specifica il nome (**`name`**), come **`apc`**, ed un numero di porta APC switch power unico (**`port`**) per ogni nodo. Per esempio, il numero di porta per node-01.example.com è **`1`** (**`port="1"`**). Il nome del dispositivo per ogni nodo (**`device name="apc"`**) indica il dispositivo di fencing usando il nome (**`name`**) di **`apc`** nella riga dell'elemento **`fencedevices`**: **`fencedevice agent="fence_apc" ipaddr="apc_ip_example" login="login_example" name="apc" passwd="password_example"/`**.

Esempio 7.5. `cluster.conf`: Metodi di fencing multipli per nodo

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
           <fence>
              <method name="APC">
                <device name="apc" port="1"/>
               </method>
              <method name="SAN">
        <device name="sanswitch1" port="11"/>
               </method>
           </fence>
           <unfence>
               <device name="sanswitch1" port="11" action="on"/>
           </unfence
```

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

Esempio 7.6. `cluster.conf`: Fencing, Porte multiple Multipath

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
      <clusternode name="node-01.example.com" nodeid="1">
          <fence>
             <method name="SAN-multi">
        <device name="sanswitch1" port="11"/>
        <device name="sanswitch2" port="11"/>
      </method>
          </fence>
          <unfence>
              <device name="sanswitch1" port="11" action="on"/>
```

```
            <device name="sanswitch2" port="11" action="on"/>
        </unfence>
    </clusternode>
    <clusternode name="node-02.example.com" nodeid="2">
        <fence>
           <method name="SAN-multi">
      <device name="sanswitch1" port="12"/>
      <device name="sanswitch2" port="12"/>
           </method>
        </fence>
        <unfence>
            <device name="sanswitch1" port="12" action="on"/>
            <device name="sanswitch2" port="12" action="on"/>
        </unfence
    </clusternode>
    <clusternode name="node-03.example.com" nodeid="3">
        <fence>
           <method name="SAN-multi">
      <device name="sanswitch1" port="13"/>
      <device name="sanswitch2" port="13"/>
           </method>
        </fence>
        <unfence>
            <device name="sanswitch1" port="13" action="on"/>
            <device name="sanswitch2" port="13" action="on"/>
        </unfence
    </clusternode>
  </clusternodes>
  <fencedevices>
       <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
       <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch2" passwd="password_example"/>
  </fencedevices>
  <rm>
  </rm>
</cluster>
```

Esempio 7.7. `cluster.conf`: Nodi per il fencing con gruppo di alimentazione doppio

```
<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>
```

Se si utilizzano gli interruttori per isolare i nodi con un gruppo di alimentazione doppio è necessario indicare agli agenti di disabilitare entrambe le porte prima di ripristinare l'alimentazione per le porte in questione. Il comportamento predefinito off-on dell'agente potrebbe non disabilitare correttamente l'alimentazione del nodo.

7.4. CONFIGURAZIONE DEI DOMINI DI FAILOVER

Un dominio di failover è un insieme specifico di nodi del cluster in grado di eseguire un servizio in presenza di un nodo fallito. Il dominio di failover può avere le seguenti caratteristiche:

- Unrestricted — Permette all'utente di specificare un insieme di membri preferiti e di indicare altresì che un servizio del cluster assegnato a questo dominio può essere eseguito su qualsiasi membro disponibile.
- Restricted — Permette all'utente di limitare i membri in grado di eseguire un servizio particolare. Se nessuno dei membri di un dominio di failover limitato è disponibile, il servizio non potrà essere avviato (sia manualmente che dal software del cluster).

- Unordered — Quando un servizio viene assegnato ad un dominio di failover non ordinato, il membro sul quale il servizio viene eseguito verrà selezionato dal gruppo di membri disponibili nel dominio di failover senza seguire alcuna priorità.
- Ordered — Permette all'utente di specificare un ordine preferito tra i membri di un dominio di failover. I domini di failover ordinati prima selezionano il numero di priorità più basso. Quindi il dominio di failover con una priorità "1" indica la priorità più alta e quindi il nodo preferito in un dominio di failover. A seguire il nodo preferito sarà quello con un numero di priorità più alto e così via.
- Failback — Permette all'utente di specificare se un servizio in un dominio di failover deve essere passato sul nodo sul quale era in esecuzione originariamente prima del suo fallimento. La configurazione di questa funzione è utile in casi in cui un nodo fallisce ripetutamente ed è parte di un dominio di failover ordinato. In tal caso se un nodo è il nodo preferito in un dominio di failover sarà possibile passare il servizio tra il nodo preferito ed un altro nodo. Questa impostazione impatta negativamente sulle prestazioni.

NOTA

La caratteristica di failback è applicabile solo se è stato configurato il failover ordinato.

NOTA

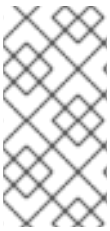
La modifica della configurazione di un dominio di failover non ha alcun effetto sui servizi attualmente in esecuzione.

NOTA

I domini di failover *non* sono necessari per un normale funzionamento.

Per impostazione predefinita i domini di failover non sono limitati ne ordinati.

In un cluster con numerosi membri l'uso di un dominio di failover limitato potrebbe ridurre il compito per l'impostazione del cluster per l'esecuzione di un servizio (come ad esempio **`httpd`**), il quale necessita di una impostazione identica della configurazione su tutti i membri che eseguono il servizio del cluster. Al posto di impostare l'intero cluster in modo da eseguire il servizio sarà necessario impostare solo i membri nel dominio di failover limitato associati con il servizio del cluster.



NOTA

Per configurare un membro preferito creare un dominio di failover non limitato che comprende un solo membro del cluster. Così facendo il servizio del cluster verrà eseguito principalmente sul membro (il membro preferito), permettendo anche di eseguire il failover del servizio del cluster su qualsiasi altro membro.

Per configurare un dominio di failover seguire le procedure di seguito indicate:

1. Aprire **`/etc/cluster/cluster.conf`** su qualsiasi nodo nel cluster.
2. Aggiungere la seguente struttura della sezione all'interno dell'elemento **`rm`** per ogni dominio di failover usato:

```
        <failoverdomains>
            <failoverdomain name="" nofailback="" ordered=""
restricted="">
                <failoverdomainnode name="" priority=""/>
                <failoverdomainnode name="" priority=""/>
                <failoverdomainnode name="" priority=""/>
            </failoverdomain>
        </failoverdomains>
```

NOTA

Il numero di attributi **failoverdomainnode** dipende del numero di nodi in un dominio di failover. La struttura della sezione **failoverdomain** mostra tre elementi **failoverdomainnode** (senza specificare alcun nodo), ciò significa che sono presenti tre nodi nel dominio di failover.

3. Nella sezione **failoverdomain** fornire i valori per gli elementi e attributi. Per la descrizione degli elementi e attributi consultare la sezione *failoverdomain* dello schema del cluster. Lo schema del cluster è disponibile su **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (per esempio **/usr/share/doc/cman-3.0.12/cluster_conf.html**) su qualsiasi nodo del cluster. Per un esempio di sezione **failoverdomains** consultare Esempio 7.8, «Un dominio di failover aggiunto a **cluster.conf**».

4. Aggiornare l'attributo **config_version** aumentando il proprio valore (per esempio, modificandolo da **config_version="2"** a **config_version="3">**).

5. Salvare **/etc/cluster/cluster.conf**.

6. **(Opzionale)** Convalidare il file con lo schema del cluster (**cluster.rng**) eseguendo il comando **ccs_config_validate**. Per esempio:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Eseguire il comando **cman_tool version -r** per diffondere la configurazione al resto dei nodi del cluster.

8. Procedere alla Sezione 7.5, «Configurazione dei servizi HA».

Esempio 7.8, «Un dominio di failover aggiunto a **cluster.conf**» mostra un esempio di una configurazione con un dominio di failover non limitato e ordinato.

Esempio 7.8. Un dominio di failover aggiunto a `cluster.conf`

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
```

```
                </method>
            </fence>
        </clusternode>
        <clusternode name="node-02.example.com" nodeid="2">
            <fence>
               <method name="APC">
                 <device name="apc" port="2"/>
               </method>
            </fence>
        </clusternode>
        <clusternode name="node-03.example.com" nodeid="3">
            <fence>
               <method name="APC">
                 <device name="apc" port="3"/>
               </method>
            </fence>
        </clusternode>
    </clusternodes>
    <fencedevices>
          <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
    </fencedevices>
    <rm>
        <failoverdomains>
            <failoverdomain name="example_pri" nofailback="0"
ordered="1" restricted="0">
                <failoverdomainnode name="node-01.example.com"
priority="1"/>
                <failoverdomainnode name="node-02.example.com"
priority="2"/>
                <failoverdomainnode name="node-03.example.com"
priority="3"/>
            </failoverdomain>
        </failoverdomains>
    </rm>
</cluster>
```

La sezione **failoverdomains** contiene una sezione **failoverdomain** per ogni dominio di failover nel cluster. In questo esempio è presente un dominio di failover. Nella riga **failoverdomain** il nome (**name**) viene specificato come **example_pri**. Altresì non è specificato alcun failback (**failback="0"**), il failover è ordinato (**ordered="1"**), ed il dominio di failover non ha restrizioni (**restricted="0"**).

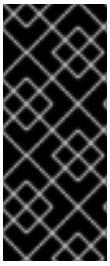
7.5. CONFIGURAZIONE DEI SERVIZI HA

La configurazione dei servizi HA (High Availability) consiste nella configurazione delle risorse e della loro assegnazione ai servizi.

Le seguenti sezioni descrivono come modificare **/etc/cluster/cluster.conf** in modo da aggiungere le risorse ed i servizi.

- Sezione 7.5.1, «Come aggiungere le risorse del cluster»

- Sezione 7.5.2, «Come aggiungere un servizio ad un cluster»



IMPORTANTE

Con i servizi e le risorse High Availability sono disponibili una vasta gamma di configurazioni. Per una migliore comprensione del comportamento delle risorse e dei parametri consultare Appendice B, *Parametri della risorsa HA* e Appendice C, *Comportamento delle risorse HA*. Per una prestazione ottimale e per il supporto della configurazione contattare un rappresentante autorizzato di Red Hat.

7.5.1. Come aggiungere le risorse del cluster

È possibile configurare due tipi di risorse:

- Globali — Risorse disponibili a qualsiasi servizio nel cluster. Esse sono configurate nella sezione **`resources`** del file di configurazione (all'interno dell'elemento **`rm`**).
- Specifico al servizio — Risorse disponibili solo ad un servizio. Esse sono configurate in ogni sezione **`service`** del file di configurazione (all'interno dell'elemento **`rm`**).

Questa sezione descrive il metodo attraverso il quale è possibile aggiungere una risorsa globale. Per le procedure sulla configurazione delle risorse specifiche al servizio consultare Sezione 7.5.2, «Come aggiungere un servizio ad un cluster».

Per aggiungere una risorsa globale del cluster seguire le fasi in questa sezione.

1. Aprire **`/etc/cluster/cluster.conf`** su qualsiasi nodo nel cluster.
2. Aggiungere una sezione **`resources`** all'interno dell'elemento **`rm`**. Per esempio:

```
    <rm>
        <resources>

        </resources>
    </rm>
```

3. Popolarla con le risorse in base ai servizi che desiderate creare. Per esempio di seguito sono riportate le risorse da usare in un servizio Apache. Esse consistono in una risorsa del file system (**`fs`**), una risorsa IP (**`ip`**) ed una risorsa Apache (**`apache`**).

```
    <rm>
        <resources>
           <fs name="web_fs" device="/dev/sdd2"
mountpoint="/var/www" fstype="ext3"/>
           <ip address="127.143.131.100" monitor_link="yes"
sleeptime="10"/>
           <apache config_file="conf/httpd.conf"
name="example_server" server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>
    </rm>
```

Esempio 7.9, «**cluster.conf** File con l'aggiunta delle risorse» mostra un esempio di un file **cluster.conf** con l'aggiunta di una sezione **resources**.

4. Aggiornare l'attributo **config_version** aumentando il proprio valore (per esempio modificandolo da **config_version="2"** a **config_version="3"**).

5. Salvare **/etc/cluster/cluster.conf**.

6. **(Opzionale)** Convalidare il file con lo schema del cluster (**cluster.rng**) eseguendo il comando **ccs_config_validate**. Per esempio:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Eseguire il comando **cman_tool version -r** per diffondere la configurazione al resto dei nodi del cluster.

8. Verificare che il file di configurazione aggiornato è stato diffuso.

9. Procedere alla Sezione 7.5.2, «Come aggiungere un servizio ad un cluster».

Esempio 7.9. cluster.conf File con l'aggiunta delle risorse

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0"
```

```
ordered="1" restricted="0">
                <failoverdomainnode name="node-01.example.com"
priority="1"/>
                <failoverdomainnode name="node-02.example.com"
priority="2"/>
                <failoverdomainnode name="node-03.example.com"
priority="3"/>
            </failoverdomain>
        </failoverdomains>
        <resources>
            <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
            <ip address="127.143.131.100" monitor_link="yes"
sleeptime="10"/>
            <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
         </resources>

    </rm>
</cluster>
```

7.5.2. Come aggiungere un servizio ad un cluster

Per aggiungere un servizio al cluster seguire le fasi di questa sezione.

1. Aprire **/etc/cluster/cluster.conf** su qualsiasi nodo nel cluster.
2. Aggiungere una sezione **service** all'interno dell'elemento **rm** per ogni servizio. Per esempio:

```
    <rm>
        <service autostart="1" domain="" exclusive="0" name=""
recovery="restart">

        </service>
    </rm>
```

3. Configurare i seguenti parametri (attributi) nell'elemento **service**:
   - **autostart** — Specifica se eseguire un avvio automatizzato del servizio all'avvio del cluster. Usare '1' per abilitare e '0' per disabilitare; l'impostazione predefinita è abilitato.
   - **domain** — Specifica un dominio di failover (se necessario).
   - **exclusive** — Specifica una politica in cui il servizio viene eseguito solo su nodi sprovvisti di altri servizi.
   - **recovery** — Specifica una politica di ripristino del servizio. Usare le opzioni per riposizionare, riavviare e riavviare-disabilitare il servizio.
4. In base al tipo di risorse da usare popolate il servizio con risorse globali o specifiche al servizio.

Per esempio ecco riportato un servizio Apache che utilizza risorse globali:

```
    <rm>
        <resources>
                <fs name="web_fs" device="/dev/sdd2"
mountpoint="/var/www" fstype="ext3"/>
                <ip address="127.143.131.100" monitor_link="yes"
sleeptime="10"/>
                <apache config_file="conf/httpd.conf"
name="example_server" server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>
        <service autostart="1" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
                <fs ref="web_fs"/>
                <ip ref="127.143.131.100"/>
                <apache ref="example_server"/>
        </service>
    </rm>
```

Esempio di un servizio Apache che utilizza risorse specifiche al servizio:

```
    <rm>
        <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
                <fs name="web_fs2" device="/dev/sdd3"
mountpoint="/var/www2" fstype="ext3"/>
                <ip address="127.143.131.101" monitor_link="yes"
sleeptime="10"/>
                <apache config_file="conf/httpd.conf"
name="example_server2" server_root="/etc/httpd" shutdown_wait="0"/>
        </service>
    </rm>
```

Esempio 7.10, «**cluster.conf** con l'aggiunta dei servizi: Usando le risorse globali e le risorse specifiche al servizio» mostra un esempio di file **cluster.conf** con due servizi:

- **example_apache** — Questo servizio utilizza le risorse globali **web_fs**, **127.143.131.100**, e **example_server**.
- **example_apache2** — Questo servizio utilizza risorse specifiche del servizio **web_fs2**, **127.143.131.101**, e **example_server2**.

5. Aggiornare l'attributo **config_version** aumentando il proprio valore (per esempio, modificandolo da **config_version="2"** a **config_version="3">**).
6. Salvare **/etc/cluster/cluster.conf**.
7. **(Opzionale)** Convalidare il file aggiornato con lo schema del cluster (**cluster.rng**) eseguendo il comando **ccs_config_validate**. Per esempio:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

8. Eseguire il comando **`cman_tool version -r`** per diffondere la configurazione al resto dei nodi del cluster.

9. Verificare che il file di configurazione aggiornato è stato diffuso.

10. Procedere alla Sezione 7.8, «Verifica di una configurazione».

Esempio 7.10. `cluster.conf` con l'aggiunta dei servizi: Usando le risorse globali e le risorse specifiche al servizio

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0"
ordered="1" restricted="0">
               <failoverdomainnode name="node-01.example.com"
priority="1"/>
               <failoverdomainnode name="node-02.example.com"
priority="2"/>
               <failoverdomainnode name="node-03.example.com"
priority="3"/>
           </failoverdomain>
       </failoverdomains>
       <resources>
```

```
            <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
            <ip address="127.143.131.100" monitor_link="yes"
sleeptime="10"/>
            <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>
        <service autostart="1" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
            <fs ref="web_fs"/>
            <ip ref="127.143.131.100"/>
            <apache ref="example_server"/>
        </service>
        <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
            <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www2"
fstype="ext3"/>
            <ip address="127.143.131.101" monitor_link="yes"
sleeptime="10"/>
            <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
        </service>
    </rm>
</cluster>
```

7.6. CONFIGURAZIONE PROTOCOLLO RING RIDONDANTE

Con Red Hat Enterprise Linux 6.4, Red Hat High Availability Add-On rende disponibile il supporto per la configurazione del protocollo ring ridondante.

Durante la configurazione di un sistema all'uso del protocollo ring ridondante è consigliato considerare i seguenti fattori:

- Non specificare più idi due ring.
- Ogni ring deve usare lo stesso protocollo; non usare un mix tra IPv4 e IPv6.
- Se necessario specificare manualmente un indirizzo multicast per il secondo ring. Se specificate un indirizzo multicast per il secondo ring, l'indirizzo o la porta alternativi devono essere diversi dall'indirizzo multicast per il primo ring. Se non specificate un indirizzo alternativo per il secondo ring il sistema userà automaticamente un indirizzo multicast diverso.

  Se specificate una porta alternativa i numeri della porta del primo ring ed il numero del secondo ring devono differire di almeno due unità poichè il sistema utilizza il numero della porta e porta-1 per eseguire le sue operazioni.
- Non utilizzate due interfacce diverse sulla stessa sottorete.
- In generale è consigliato configurare un protocollo ring ridondante su due NIC diversi, e due interruttori, nel caso di un fallimento di uno dei due NIC o di un interruttore.
- Non usare **`ifdown`** o **`service network stop`** per simulare il fallimento della rete, poichè così facendo verrà distrutto l'intero cluster. Per il ripristino del cluster sarà necessario il riavvio di tutti i nodi.

- Non utilizzate **NetworkManager** poichè così facendo verrà eseguito il comando **ifdown** se il cavo non è collegato.
- Se un nodo del NIC fallisce l'intero ring sarà contrassegnato come fallito.
- In presenza di un ring fallito non sarà necessario eseguire alcun intervento manuale. Per il ripristino correggere l'origine dell'errore, in questo caso l'interruttore o il NIC fallito.

Per specificare una seconda interfaccia di rete per l'utilizzo di un protocollo ring ridondante, aggiungere un componente **altname** nella sezione **clusternode** del file di configurazione **cluster.conf**. Quando specificate **altname** sarà necessario specificare un attributo **name** per indicare il nome di un secondo host o indirizzo IP per il nodo.

Il seguente esempio specifica **clusternet-node1-eth2** come nome alternativo per il nodo del cluster **clusternet-node1-eth1**.

```
<cluster name="mycluster" config_version="3" >
  <logging debug="on"/>
  <clusternodes>
    <clusternode name="clusternet-node1-eth1" votes="1" nodeid="1">
      <fence>
        <method name="single">
          <device name="xvm" domain="clusternet-node1"/>
        </method>
      </fence>
      <altname name="clusternet-node1-eth2"/>
    </clusternode>
```

La sezione **altname** all'interno del blocco **clusternode** non dipende dalla posizione. Essa può trovarsi prima o dopo la sezione **fence**. Non specificate più di un componente **altname** per un nodo del cluster, poichè così facendo il sistema non sarà in grado di eseguire il riavvio.

Facoltativamente specificare manualmente un indirizzo multicast, una porta, ed un TTL per il secondo ring includendo un componente **altmulticast** nella sezione **cman** del file di configurazione **cluster.conf**. Il componente **altmulticast** accetta un parametro **addr**, **port** e **ttl** .

Il seguente esempio mostra la sezione **cman** di un file di configurazione del cluster, nella quale vengono impostati un indirizzo multicast, una porta ed un TTL per il secondo ring.

```
<cman>
   <multicast addr="239.192.99.73" port="666" ttl="2"/>
   <altmulticast addr="239.192.99.88" port="888" ttl="3"/>
</cman>
```

7.7. CONFIGURAZIONE DELLE OPZIONI DI DEBUG

È possibile abilitare il debugging per tutti i demoni in un cluster oppure la registrazione per processazioni del cluster specifiche.

Per abilitare il debugging per tutti i demoni aggiungere il seguente su **/etc/cluster/cluster.conf**. Per impostazione predefinita la registrazione viene eseguita su **/var/log/cluster/*daemon*.log**.

```
<cluster config_version="7" name="rh6cluster">
  <logging debug="on"/>
   ...
</cluster>
```

Per abilitare il debugging per processi individuali del cluster aggiungere le seguenti righe al file **/etc/cluster/cluster.conf**. La configurazione della registrazione per-demone sovrascrive le impostazioni globali.

```
<cluster config_version="7" name="rh6cluster">
   ...
  <logging>
       <!-- turning on per-subsystem debug logging -->
       <logging_daemon name="corosync" debug="on" />
       <logging_daemon name="fenced" debug="on" />
       <logging_daemon name="qdiskd" debug="on" />
       <logging_daemon name="rgmanager" debug="on" />
       <logging_daemon name="dlm_controld" debug="on" />
       <logging_daemon name="gfs_controld" debug="on" />
  </logging>
   ...
</cluster>
```

Per un elenco dei demoni per i quali è possibile abilitare la registrazione insieme alle opzioni aggiuntive per una registrazione per-demone e globale, consultare la pagina man di **cluster.conf**(5).

7.8. VERIFICA DI UNA CONFIGURAZIONE

Una volta creato il file di configurazione del cluster verificare che lo stesso sia in esecuzione eseguendo le seguenti fasi:

1. Su ogni nodo riavviare il software del cluster. Tale azione assicura che qualsiasi modifica fatta alla configurazione e controllata solo al momento dell'avvio, sia inclusa durante la normale esecuzione della configurazione stessa. Riavviare il software del cluster eseguendo **service cman restart**. Per esempio:

   ```
   [root@example-01 ~]# service cman restart
   Stopping cluster:
      Leaving fence domain...                                 [  OK
   ]
      Stopping gfs_controld...                                [  OK
   ]
      Stopping dlm_controld...                                [  OK
   ]
      Stopping fenced...                                      [  OK
   ]
      Stopping cman...                                        [  OK
   ```

```
]
   Waiting for corosync to shutdown:                          [  OK  ]
   Unloading kernel modules...                                [  OK
]
   Unmounting configfs...                                     [  OK
]
Starting cluster:
   Checking Network Manager...                                [  OK
]
   Global setup...                                            [  OK
]
   Loading kernel modules...                                  [  OK
]
   Mounting configfs...                                       [  OK
]
   Starting cman...                                           [  OK
]
   Waiting for quorum...                                      [  OK
]
   Starting fenced...                                         [  OK
]
   Starting dlm_controld...                                   [  OK
]
   Starting gfs_controld...                                   [  OK
]
   Unfencing self...                                          [  OK
]
   Joining fence domain...                                    [  OK
]
```

2. Eseguire **`service clvmd start`** se CLVM è stato usato per creare i volumi clusterizzati. Per esempio:

```
[root@example-01 ~]# service clvmd start
Activating VGs:                                               [  OK
]
```

3. Eseguire **`service gfs2 start`** se state usando Red Hat GFS2. Per esempio:

```
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                         [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                         [  OK  ]
```

4. Eseguire **`service rgmanager start`** se usate i servizi high-availability (HA). Per esempio:

```
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                             [  OK  ]
```

5. Su ogni nodo del cluster eseguire **`cman_tools nodes`** per verificare che i nodi siano membri attivi del cluster (contrassegnati con "M" nella colonna dello stato, "Sts"). Per esempio:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
```

```
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

6. Su qualsiasi nodo, utilizzando l'utilità **clustat**, verificate che i servizi HA siano in esecuzione come previsto. In aggiunta **clustat** mostra lo stato dei nodi del cluster. Per esempio:

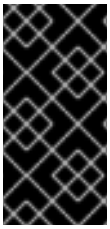
```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local,
rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    --
---
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)
disabled
```

7. Se il cluster è in esecuzione come previsto, il processo di creazione del file di configurazione sarà terminato. Sarà possibile gestire il cluster con i tool della linea di comando descritti in Capitolo 8, *Gestione di Red Hat High Availability Add-On con i tool della linea di comando*.

CAPITOLO 8. GESTIONE DI RED HAT HIGH AVAILABILITY ADD-ON CON I TOOL DELLA LINEA DI COMANDO

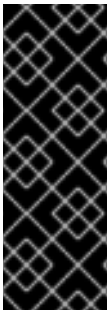
Questo capitolo descrive i vari compiti amministrativi per la gestione di Red Hat High Availability Add-On e consiste nelle seguenti sezioni:

- Sezione 8.1, «Avvio ed arresto del software del cluster»
- Sezione 8.2, «Rimozione o aggiunta di un nodo»
- Sezione 8.3, «Gestione servizi ad elevata disponibilità»
- Sezione 8.4, «Aggiornamento di una configurazione»



IMPORTANTE

Assicuratevi che l'implementazione di Red Hat High Availability Add-On possa essere supportata ed in grado di soddisfare i vostri requisiti. Consultate un rappresentante autorizzato di Red Hat per una verifica della configurazione prima dell'impiego. In aggiunta assegnate un periodo di prova per le varie modalità d'errore.



IMPORTANTE

Questo capitolo fa riferimento ad attributi ed elementi **`cluster.conf`** comunemente usati. Per un elenco completo ed una descrizione degli elementi ed attributi di **`cluster.conf`**, consultate lo schema disponibile su **`/usr/share/cluster/cluster.rng`**, **`/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html`** (per esempio **`/usr/share/doc/cman-3.0.12/cluster_conf.html`**).

IMPORTANTE

Alcune procedure in questo capitolo richiedono l'uso del comando **`cman_tool version -r`** per diffondere la configurazione all'interno di un cluster. L'utilizzo di questo comando richiede l'esecuzione di **`ricci`**.

NOTA

Le procedure presenti in questo capitolo possono includere comandi specifici per alcuni tool della linea di comando elencati in Appendice E, *Sommario dei tool della linea di comando*. Per maggiori informazioni sui comandi e sulle variabili consultare la pagina man do ogni tool della linea di comando.

8.1. AVVIO ED ARRESTO DEL SOFTWARE DEL CLUSTER

È possibile avviare o arrestare il software del cluster su di un nodo in base alla Sezione 8.1.1, «Avvio del software del cluster» e Sezione 8.1.2, «Arresto del software del cluster». L'avvio del software su un nodo causa l'ingresso del nodo nel cluster; l'arresto del software su di un nodo causa l'esclusione dello stesso dal cluster.

8.1.1. Avvio del software del cluster

Per avviare il software del cluster su un nodo digitare i seguenti comandi nell'ordine riportato:

1. **`service cman start`**
2. **`service clvmd start`**, se CLVM è stato usato per creare volumi clusterizzati
3. **`service gfs2 start`**, se usate Red Hat GFS2
4. **`service rgmanager start`**, se usate i servizi high-availability (HA) (**`rgmanager`**).

Per esempio:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                                [  OK  ]
   Global setup...                                            [  OK  ]
   Loading kernel modules...                                  [  OK  ]
   Mounting configfs...                                       [  OK  ]
   Starting cman...                                           [  OK  ]
   Waiting for quorum...                                      [  OK  ]
   Starting fenced...                                         [  OK  ]
   Starting dlm_controld...                                   [  OK  ]
   Starting gfs_controld...                                   [  OK  ]
   Unfencing self...                                          [  OK  ]
   Joining fence domain...                                    [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                               [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example" now
active
                                                              [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                         [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                         [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                             [  OK  ]
[root@example-01 ~]#
```

8.1.2. Arresto del software del cluster

Per arrestare il software su un nodo digitare i seguenti comandi nell'ordine riportato:

1. **`service rgmanager stop`**, se utilizzate i servizi high-availability (HA) (**`rgmanager`**).
2. **`service gfs2 stop`**, se utilizzate Red Hat GFS2
3. **`umount -at gfs2`**, se utilizzate Red Hat GFS2 insieme al **`rgmanager`**, per assicurare che qualsiasi file GFS2 montato durante l'avvio di **`rgmanager`** (ma non smontato durante l'arresto) sia stato smontato.
4. **`service clvmd stop`**, se CLVM è stato usato per creare volumi clusterizzati
5. **`service cman stop`**

Per esempio:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# umount -at gfs2
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

NOTA

L'arresto del software del cluster su un nodo causerà il failover del servizi HA su un altro nodo. Un'alternativa a tale processo è il riposizionamento o la migrazione dei servizi HA su un altro nodo prima di arrestare il software. Per informazioni sulla gestione dei servizi HA consultate Sezione 8.3, «Gestione servizi ad elevata disponibilità».

8.2. RIMOZIONE O AGGIUNTA DI UN NODO

Questa sezione mostra come rimuovere ed aggiungere un nodo nel cluster. Per rimuovere un nodo dal cluster consultare Sezione 8.2.1, «Rimozione di un nodo dal cluster»; per aggiungere un nodo al cluster consultare Sezione 8.2.2, «Come aggiungere un nodo al cluster».

8.2.1. Rimozione di un nodo dal cluster

Il processo di rimozione del nodo dal cluster consiste nell'arrestare il software del cluster sul nodo che si desidera rimuovere ed aggiornare la configurazione del cluster in modo da riflettere la modifica apportata.

IMPORTANTE

Se la rimozione del cluster causa una transizione da un cluster con più nodi ad uno con due nodi sarà necessario riavviare il software del cluster su ogni nodo dopo aver aggiornato il file di configurazione del cluster.

Per rimuovere un nodo dal cluster eseguire le fasi di seguito riportate:

1. Su qualsiasi nodo usare l'utilità **clusvcadm** per riposizionare, migrare o arrestare ogni servizio HA in esecuzione sul nodo rimosso dal cluster. Per informazioni sull'uso di **clusvcadm** consultare la Sezione 8.3, «Gestione servizi ad elevata disponibilità».

2. Sul nodo da rimuovere dal cluster arrestate il software consultando Sezione 8.1.2, «Arresto del software del cluster». Per esempio:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK
]
clvmd terminated                                           [  OK
]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK
]
   Stopping gfs_controld...                                [  OK
]
   Stopping dlm_controld...                                [  OK
]
   Stopping fenced...                                      [  OK
]
   Stopping cman...                                        [  OK
]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK
]
   Unmounting configfs...                                  [  OK
]
[root@example-01 ~]#
```

3. Su qualsiasi nodo nel cluster modificare **/etc/cluster/cluster.conf** in modo da rimuovere la sezione **clusternode** del nodo da cancellare. Per esempio, in Esempio 8.1, «Configurazione cluster a tre nodi», se node-03.example.com deve essere rimosso, allora cancellate la sezione **clusternode** per quel nodo. Se la rimozione di un nodo (o nodi) causerà la presenza di soli due nodi nel cluster, aggiungere la seguente riga al file di configurazione in modo da permettere ad un singolo nodo di mantenere il quorum (per esempio se un nodo fallisce):

   <cman two_node="1" expected_votes="1"/>

   Consultate Sezione 8.2.3, «Esempi di configurazione a due e tre nodi» per un confronto tra una configurazione a tre nodi ed una a due nodi.

4. Aggiornare l'attributo **config_version** aumentando il proprio valore (per esempio, modificandolo da **config_version="2"** a **config_version="3">**).

5. Salvare **/etc/cluster/cluster.conf**.

6. **(Opzionale)** Convalidare il file aggiornato con lo schema del cluster (**cluster.rng**) eseguendo il comando **ccs_config_validate**. Per esempio:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Eseguire il comando **`cman_tool version -r`** per diffondere la configurazione al resto dei nodi del cluster.

8. Verificare che il file di configurazione aggiornato è stato diffuso.

9. Se contando i nodi sarete in presenza di un cluster con solo due nodi, allora sarà necessario riavviare il software del cluster nel modo seguente:

   1. Su ogni nodo arrestate il software del cluster consultando Sezione 8.1.2, «Arresto del software del cluster». Per esempio:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK
]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK
]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK
]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [
OK  ]
clvmd terminated                                           [
OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [
OK  ]
   Stopping gfs_controld...                                [
OK  ]
   Stopping dlm_controld...                                [
OK  ]
   Stopping fenced...                                      [
OK  ]
   Stopping cman...                                        [
OK  ]
   Waiting for corosync to shutdown:                       [  OK
]
   Unloading kernel modules...                             [
OK  ]
   Unmounting configfs...                                  [
OK  ]
[root@example-01 ~]#
```

   2. Su ogni nodo avviate il software del cluster consultando Sezione 8.1.1, «Avvio del software del cluster». Per esempio:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [
OK  ]
   Global setup...                                         [
OK  ]
   Loading kernel modules...                               [
OK  ]
   Mounting configfs...                                    [
```

```
OK  ]
   Starting cman...                                        [
OK  ]
   Waiting for quorum...                                   [
OK  ]
   Starting fenced...                                      [
OK  ]
   Starting dlm_controld...                                [
OK  ]
   Starting gfs_controld...                                [
OK  ]
   Unfencing self...                                       [
OK  ]
   Joining fence domain...                                 [
OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [
OK  ]
Activating VG(s):   2 logical volume(s) in volume group
"vg_example" now active
                                                           [
OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK
]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK
]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK
]
[root@example-01 ~]#
```

3. Su ogni nodo del cluster eseguire **cman_tool nodes** per verificare che i nodi siano membri attivi del cluster (contrassegnati con "M" nella colonna dello stato, "Sts"). Per esempio:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
```

4. Su qualsiasi nodo, utilizzando l'utilità **clustat**, verificate che i servizi HA siano in esecuzione come previsto. In aggiunta **clustat** mostra lo stato dei nodi del cluster. Per esempio:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local,
rgmanager
```

```
 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------
-----
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)
disabled
```

8.2.2. Come aggiungere un nodo al cluster

Per aggiungere un nodo al cluster aggiornare la configurazione del cluster, diffondere la configurazione aggiornata al nodo da aggiungere ed avviare il software sul nodo. A tale scopo eseguire le fasi di seguito riportate:

1. Su qualsiasi nodo nel cluster modificare **`/etc/cluster/cluster.conf`** in modo da aggiungere una sezione **`clusternode`** per il nodo che deve essere aggiunto. Per esempio, in Esempio 8.2, «Configurazione cluster a due nodi», se node-03.example.com deve essere aggiunto, allora aggiungere la sezione **`clusternode`** per quel nodo. Se con l'aggiunta di un nodo (o nodi) il cluster passerà da due a tre o più nodi, rimuovere i seguenti attributi **`cman`** da **`/etc/cluster/cluster.conf`**:

   - **`cman two_node="1"`**
   - **`expected_votes="1"`**

   Consultate Sezione 8.2.3, «Esempi di configurazione a due e tre nodi» per un confronto tra una configurazione a tre nodi ed una a due nodi.

2. Aggiornare l'attributo **`config_version`** aumentando il proprio valore (per esempio, modificandolo da **`config_version="2"`** a **`config_version="3">`**).

3. Salvare **`/etc/cluster/cluster.conf`**.

4. **`(Opzionale)`** Convalidare il file aggiornato con lo schema del cluster (**`cluster.rng`**) eseguendo il comando **`ccs_config_validate`**. Per esempio:

   ```
   [root@example-01 ~]# ccs_config_validate
   Configuration validates
   ```

5. Eseguire il comando **`cman_tool version -r`** per diffondere la configurazione al resto dei nodi del cluster.

6. Verificare che il file di configurazione aggiornato è stato diffuso.

7. Diffondere il file di configurazione aggiornato su **`/etc/cluster/`** in ogni nodo da aggiungere al cluster. Per esempio usare il comando **`scp`** per inviare il file di configurazione aggiornato ad ogni nodo da aggiungere al cluster.

8. Se contando i nodi il cluster è passato da due ad un numero di nodi maggiore allora sarà necessario riavviare il software del cluster nel modo seguente:

   1. Su ogni nodo arrestate il software del cluster consultando Sezione 8.1.2, «Arresto del software del cluster». Per esempio:

      ■

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK
]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK
]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK
]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [
OK  ]
clvmd terminated                                           [
OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [
OK  ]
   Stopping gfs_controld...                                [
OK  ]
   Stopping dlm_controld...                                [
OK  ]
   Stopping fenced...                                      [
OK  ]
   Stopping cman...                                        [
OK  ]
   Waiting for corosync to shutdown:                       [  OK
]
   Unloading kernel modules...                             [
OK  ]
   Unmounting configfs...                                  [
OK  ]
[root@example-01 ~]#
```

2. Su ogni nodo avviate il software del cluster consultando Sezione 8.1.1, «Avvio del software del cluster». Per esempio:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [
OK  ]
   Global setup...                                         [
OK  ]
   Loading kernel modules...                               [
OK  ]
   Mounting configfs...                                    [
OK  ]
   Starting cman...                                        [
OK  ]
   Waiting for quorum...                                   [
OK  ]
   Starting fenced...                                      [
OK  ]
   Starting dlm_controld...                                [
OK  ]
   Starting gfs_controld...                                [
OK  ]
```

```
   Unfencing self...                                       [
OK  ]
   Joining fence domain...                                 [
OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [
OK  ]
Activating VG(s):   2 logical volume(s) in volume group
"vg_example" now active
                                                           [
OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK
]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK
]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK
]
[root@example-01 ~]#
```

9. Ad ogni nodo da aggiungere al cluster avviare il software del cluster in base alla Sezione 8.1.1, «Avvio del software del cluster». Per esempio:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK
]
   Global setup...                                         [  OK
]
   Loading kernel modules...                               [  OK
]
   Mounting configfs...                                    [  OK
]
   Starting cman...                                        [  OK
]
   Waiting for quorum...                                   [  OK
]
   Starting fenced...                                      [  OK
]
   Starting dlm_controld...                                [  OK
]
   Starting gfs_controld...                                [  OK
]
   Unfencing self...                                       [  OK
]
   Joining fence domain...                                 [  OK
]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK
]
Activating VG(s):   2 logical volume(s) in volume group "vg_example"
now active
                                                           [  OK
]
[root@example-01 ~]# service gfs2 start
```

```
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]

[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

10. Usando l'utilità **clustat**, verificare che ogni nodo aggiunto sia parte del cluster ed in esecuzione: Per esempio:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local,
rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    --
---
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)
disabled
```

Per informazioni sull'uso di **clustat** consultare Sezione 8.3, «Gestione servizi ad elevata disponibilità».

Usare altresì **cman_tool status** per verificare il conteggio del quorum ed i voti ed il conteggio dei nodi. Per esempio:

```
[root@example-01 ~]#cman_tool status
Version: 6.2.0
Config Version: 19
Cluster Name: mycluster
Cluster Id: 3794
Cluster Member: Yes
Cluster Generation: 548
Membership state: Cluster-Member
Nodes: 3
Expected votes: 3
Total votes: 3
Node votes: 1
Quorum: 2
Active subsystems: 9
Flags:
Ports Bound: 0 11 177
Node name: node-01.example.com
```

```
Node ID: 3
Multicast addresses: 239.192.14.224
Node addresses: 10.15.90.58
```

11. Su qualsiasi nodo usare l'utilità **clusvcadm** per riposizionare o migrare un servizio in esecuzione su un nuovo nodo del cluster. Sarà altresì possibile abilitare o disabilitare qualsiasi servizio. Per informazioni sull'uso di **clusvcadm** consultare la Sezione 8.3, «Gestione servizi ad elevata disponibilità»

8.2.3. Esempi di configurazione a due e tre nodi

Consultare gli esempi seguenti per un confronto tra configurazioni a due e tre nodi.

Esempio 8.1. Configurazione cluster a tre nodi

```
<cluster name="mycluster" config_version="3">
   <cman/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0"
ordered="1" restricted="0">
               <failoverdomainnode name="node-01.example.com"
priority="1"/>
               <failoverdomainnode name="node-02.example.com"
priority="2"/>
               <failoverdomainnode name="node-03.example.com"
priority="3"/>
```

```
            </failoverdomain>
        </failoverdomains>
        <resources>
            <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
            <ip address="127.143.131.100" monitor_link="yes"
sleeptime="10"/>
            <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>
        <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
            <fs ref="web_fs"/>
            <ip ref="127.143.131.100"/>
            <apache ref="example_server"/>
        </service>
        <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
            <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www"
fstype="ext3"/>
            <ip address="127.143.131.101" monitor_link="yes"
sleeptime="10"/>
            <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
        </service>
    </rm>
</cluster>
```

Esempio 8.2. Configurazione cluster a due nodi

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

```
        <failoverdomains>
            <failoverdomain name="example_pri" nofailback="0"
ordered="1" restricted="0">
                <failoverdomainnode name="node-01.example.com"
priority="1"/>
                <failoverdomainnode name="node-02.example.com"
priority="2"/>
            </failoverdomain>
        </failoverdomains>
        <resources>
            <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
            <ip address="127.143.131.100" monitor_link="yes"
sleeptime="10"/>
            <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>
        <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
            <fs ref="web_fs"/>
            <ip ref="127.143.131.100"/>
            <apache ref="example_server"/>
        </service>
        <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
            <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www"
fstype="ext3"/>
            <ip address="127.143.131.101" monitor_link="yes"
sleeptime="10"/>
            <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
        </service>
    </rm>
</cluster>
```

8.3. GESTIONE SERVIZI AD ELEVATA DISPONIBILITÀ

È possibile gestire i servizi ad elevata disponibilità usando **Cluster Status Utility**, **`clustat`**, ed il **Cluster User Service Administration Utility**, **`clusvcadm`**. **`clustat`** visualizza lo stato di un cluster e **`clusvcadm`** fornisce i mezzi necessari per gestire i servizi ad elevata disponibilità.

Questa sezione fornisce le informazioni di base sulla gestione dei servizi HA usando **`clustat`** e **`clusvcadm`**. Essa consiste nelle seguenti sottosezioni:

- Sezione 8.3.1, «Visualizzazione dello stato dei servizi HA con **`clustat`**»
- Sezione 8.3.2, «Gestione dei servizi HA con **`clusvcadm`**»

8.3.1. Visualizzazione dello stato dei servizi HA con `clustat`

`clustat` mostra lo stato dell'intero cluster. Esso è in grado di mostrare le informazioni relative all'appartenenza, fornisce una visuale sul quorum, uno stato di tutti i servizi ad elevata disponibilità ed

indica su quale nodo viene eseguito il comando **clustat** (Locale). Tabella 8.1, «Stato dei servizi» descrive lo stato dei servizi e possono essere visualizzati con l'esecuzione di **clustat**. Esempio 8.3, «Visualizzazione del comando **clustat**» mostra un esempio di un riporto **clustat**. Per informazioni dettagliate su come eseguire il comando **clustat** consultare la pagina man di **clustat**.

Tabella 8.1. Stato dei servizi

Stato dei servizi	Descrizione
Started	Le risorse del servizio sono state configurate e sono disponibili sul sistema del cluster che possiede il servizio.
Recovering	Il servizio è in attesa dell'avvio su un altro nodo.
Disabled	Il servizio è stato disabilitato e non è stato assegnato alcun proprietario. Un servizio disabilitato non viene mai riavviato automaticamente dal cluster.
Stopped	In questo stato il servizio verrà preso in considerazione per l'avvio dopo la successiva transizione del nodo o del servizio. Questo è uno stato provvisorio. Da questo stato è possibile disabilitare o abilitare il servizio.
Failed	Si presume che il servizio sia terminato. Un servizio viene impostato su questo stato ogni qualvolta una operazione di *arresto* fallisce. Dopo aver posizionato il servizio su questo stato verificare che non vi sia alcuna risorsa assegnata (per esempio file system montato) prima di emettere una richiesta **disable**. La sola operazione che si può intraprendere quando un servizio presenta il suddetto stato è **disable**.
Uninitialized	Questo stato può essere visualizzato in determinati casi durante l'avvio e l'esecuzione di **clustat -f**.

Esempio 8.3. Visualizzazione del comando clustat

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:15 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local,
rgmanager

 Service Name                   Owner (Last)                   State
 ------- ----                   ----- ------                   -----
 service:example_apache         node-01.example.com            started
 service:example_apache2        (none)
disabled
```

8.3.2. Gestione dei servizi HA con `clusvcadm`

È possibile gestire i servizi HA usando il comando **`clusvcadm`**. Con esso sarà possibile eseguire le seguenti operazioni:

- Abilitare ed avviare un servizio.
- Disabilitare un servizio.
- Arrestare un servizio.
- Eseguire il freeze di un servizio
- Eseguire l'unfreeze di un servizio
- Migrare un servizio (solo per i servizi della macchina virtuale)
- Riposizionare un servizio.
- Riavviare un servizio.

Tabella 8.2, «Funzioni del servizio» descrive le operazioni in modo dettagliato. Per una descrizione completa su come eseguire le suddette operazioni consultare la pagina man dell'utilità **`clusvcadm`**.

Tabella 8.2. Funzioni del servizio

Funzione del servizio	Descrizione	Sintassi del comando
Enable	Avvia il servizio facoltativamente su di una destinazione preferita e in base alle regole del dominio di failover. In loro assenza l'host locale sul quale viene eseguito **`clusvcadm`** avvierà il servizio. Se il processo *d'avvio* fallisce il servizio si comporta come se fosse stata richiesta una operazione di *riposizionamento* (consultare **Riposiziona** in questa tabella). Se l'operazione ha successo il servizio avrà uno stato started (avviato).	**`clusvcadm -e <service_name>`** o **`clusvcadm -e <service_name> -m <member>`** (Con l'uso dell'opzione -m verrà specificato il membro di destinazione preferito sul quale avviare il servizio.)
Disable	Arresta il servizio e lo posiziona in uno stato disabled (disabilitato). Questa è l'unica operazione permessa quando un servizio è in uno stato *failed*.	**`clusvcadm -d <service_name>`**

Funzione del servizio	Descrizione	Sintassi del comando
Relocate	Sposta il servizio su un altro nodo. Facoltativamente sarà possibile specificare un nodo preferito per ricevere il servizio, ma l'impossibilità di eseguire il servizio sull'host (per esempio, se il servizio non viene avviato o se l'host è offline) non impedisce il riposizionamento e per questo motivo verrà scelto un nodo diverso. **`rgmanager`** cerca di avviare il servizio su ogni nodo disponibile sul cluster. Se nessun nodo di destinazione presente nel cluster avvia con successo il servizio, il riposizionamento fallisce e si eseguirà un tentativo di riavvio del servizio sul proprietario originario. Se il suddetto proprietario non è in grado di riavviare il servizio il servizio stesso avrà lo stato di *stopped* (arrestato).	**`clusvcadm -r <service_name>`** o **`clusvcadm -r <service_name> -m <member>`** (Con l'uso dell'opzione -m verrà specificato il membro di destinazione preferito sul quale avviare il servizio.)
Stop	Arresta il servizio e lo posiziona in uno stato *stopped*.	**`clusvcadm -s <service_name>`**
Freeze	Esegue il freeze del servizio sul nodo sul quale è in esecuzione. Tale operazione impedisce i controlli dello stato del servizio ed il failover in presenza di un nodo fallito o di un arresto di rgmanager. Può essere usato per sospendere un servizio e permettere la gestione delle risorse sottostanti. Consultate sezione chiamata «Considerazioni sull'uso delle operazioni Freeze ed Unfreeze» per informazioni rilevanti sull'uso delle operazioni di *freeze* e *unfreeze*.	**`clusvcadm -Z <service_name>`**
Unfreeze	L'operazione di Unfreeze rimuove il servizio da uno stato *freeze*. Questa operazione abilita nuovamente i controlli dello stato. Consultare sezione chiamata «Considerazioni sull'uso delle operazioni Freeze ed Unfreeze» per informazioni rilevanti sull'uso delle operazioni *freeze* e *unfreeze*.	**`clusvcadm -U <service_name>`**

Funzione del servizio	Descrizione	Sintassi del comando
Migrate	Esegue la migrazione della macchina virtuale su un altro nodo. Specificare un nodo di destinazione. In base all'errore, il fallimento del processo di migrazione potrebbe causare uno stato *failed* della macchina virtuale o in uno stato started sul proprietario originario.	**`clusvcadm -M <service_name> -m <member>`** **IMPORTANTE** Per una *migrazione* sarà necessario *specificare* un nodo di destinazione usando l'opzione **`-m <member>`**.
Restart	Riavvia un servizio sul nodo dove risulta essere in esecuzione.	**`clusvcadm -R <service_name>`**

Considerazioni sull'uso delle operazioni Freeze ed Unfreeze

Usando l'operazione *freeze* sarà possibile gestire parte dei servizi **`rgmanager`**. Per esempio se siete in possesso di un detebase ed un web server in un servizio **`rgmanager`**, sarà possibile eseguire il freeze del servizio **`rgmanager`**, arrestare il database, eseguire il mantenimento, riavviare il database ed eseguire l'operazione di unfreeze del servizio.

Quando si esegue il freeze di un servizio, esso si comporterà nel seguente modo:

- I controlli sullo *Stato* sono disabilitati.
- Le operazioni *d'avvio* sono disabilitate.
- Le operazioni *d'arresto* sono disabilitate.
- Il failover non verrà eseguito (anche se disabiliterete il proprietario del servizio).

IMPORTANTE

Se non si rispettano le suddette linee guida le risorse potrebbero essere assegnate su host multipli:

- Se si esegue il freeze del servizio *non* arrestare tutte le istanze di rgmanager a meno che non pianificate di riavviare gli host prima di riavviare rgmanager.
- *Non* eseguite l'operazione di unfreeze di un servizio fino a quando il proprietario del servizio non si unisce nuovamente al cluster e riavvia rgmanager.

8.4. AGGIORNAMENTO DI UNA CONFIGURAZIONE

L'aggiornamento del cluster consiste nella modifica del file di configurazione del cluster (**`/etc/cluster/cluster.conf`**) e nella sua diffusione su ogni nodo nel cluster. È possibile aggiornare la configurazione usando le seguenti procedure:

- Sezione 8.4.1, «Aggiornamento di una configurazione utilizzando **`cman_tool version -r`**»

- Sezione 8.4.2, «Aggiornamento di una configurazione tramite **scp**»

8.4.1. Aggiornamento di una configurazione utilizzando `cman_tool version -r`

Per l'aggiornamento della configurazione usando il comando **`cman_tool version -r`** eseguire le seguenti fasi:

1. Su qualsiasi nodo nel cluster modificare **`/etc/cluster/cluster.conf`**
2. Aggiornare l'attributo **`config_version`** aumentando il proprio valore (per esempio, modificandolo da **`config_version="2"`** a **`config_version="3">`**).
3. Salvare **`/etc/cluster/cluster.conf`**.
4. Eseguire il comando **`cman_tool version -r`** per diffondere la configurazione al resto dei nodi del cluster. Per propagare le informazioni aggiornate sulla configurazione del cluster è necessario che **`ricci`** sia in esecuzione su ogni nodo del cluster.
5. Verificare che il file di configurazione aggiornato è stato diffuso.
6. Saltare questa fase (riavvio del software del cluster) se avete apportato solo le seguenti modifiche alla configurazione:
   - Rimozione di un nodo dalla configurazione del cluster—*ad eccezione* di quando il conteggio dei nodi risulta passare da un numero maggiore di nodi ad un cluster con due nodi. Per informazioni sulla rimozione di un nodo da un cluster e su di una transizione da un numero maggiore di due ad un cluster con due nodi consultate Sezione 8.2, «Rimozione o aggiunta di un nodo».
   - Aggiungere un nodo alla configurazione del cluster—*ad eccezione* di quando il conteggio dei nodi risulta passare da un cluster con due nodi ad un cluster con più nodi. Per informazioni su come aggiungere un nodo da un cluster e su una transizione da due nodi ad un numero maggiore di nodi consultate Sezione 8.2.2, «Come aggiungere un nodo al cluster».
   - Modifiche su come i demoni registrano le informazioni.
   - Gestione VM/servizio HA (aggiunta, modifica o cancellazione).
   - Gestione risorse (aggiunta, modifica o cancellazione).
   - Gestione dominio di failover (aggiunta, modifica o cancellazione)

   In caso contrario riavviate il software del cluster nel modo seguente:

   1. Su ogni nodo arrestate il software del cluster consultando Sezione 8.1.2, «Arresto del software del cluster». Per esempio:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK
]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK
]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK
]
[root@example-01 ~]# service clvmd stop
```

```
Signaling clvmd to exit                                    [
OK  ]
clvmd terminated                                           [
OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [
OK  ]
   Stopping gfs_controld...                                [
OK  ]
   Stopping dlm_controld...                                [
OK  ]
   Stopping fenced...                                      [
OK  ]
   Stopping cman...                                        [
OK  ]
   Waiting for corosync to shutdown:                       [  OK
]
   Unloading kernel modules...                             [
OK  ]
   Unmounting configfs...                                  [
OK  ]
[root@example-01 ~]#
```

2. Su ogni nodo avviate il software del cluster consultando Sezione 8.1.1, «Avvio del software del cluster». Per esempio:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [
OK  ]
   Global setup...                                         [
OK  ]
   Loading kernel modules...                               [
OK  ]
   Mounting configfs...                                    [
OK  ]
   Starting cman...                                        [
OK  ]
   Waiting for quorum...                                   [
OK  ]
   Starting fenced...                                      [
OK  ]
   Starting dlm_controld...                                [
OK  ]
   Starting gfs_controld...                                [
OK  ]
   Unfencing self...                                       [
OK  ]
   Joining fence domain...                                 [
OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [
OK  ]
Activating VG(s):   2 logical volume(s) in volume group
"vg_example" now active
```

```
                                                           [
OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK
]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK
]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK
]
[root@example-01 ~]#
```

Il processo di arresto ed avvio del software del cluster assicura che qualsiasi modifica alla configurazione sia inclusa nella configurazione usata per l'esecuzione.

7. Su ogni nodo del cluster eseguire **cman_tool nodes** per verificare che i nodi siano membri attivi del cluster (contrassegnati con "M" nella colonna dello stato, "Sts"). Per esempio:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

8. Su qualsiasi nodo, utilizzando l'utilità **clustat**, verificate che i servizi HA siano in esecuzione come previsto. In aggiunta **clustat** mostra lo stato dei nodi del cluster. Per esempio:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local,
rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    --
---
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)
disabled
```

9. Se il cluster è in esecuzione come previsto l'aggiornamento della configurazione è completato.

8.4.2. Aggiornamento di una configurazione tramite scp

Per aggiornare la configurazione usando il comando **scp** eseguire le fasi riportate:

1. Su ogni nodo arrestate il software del cluster consultando Sezione 8.1.2, «Arresto del software del cluster». Per esempio:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK
]
clvmd terminated                                           [  OK
]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK
]
   Stopping gfs_controld...                                [  OK
]
   Stopping dlm_controld...                                [  OK
]
   Stopping fenced...                                      [  OK
]
   Stopping cman...                                        [  OK
]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK
]
   Unmounting configfs...                                  [  OK
]
[root@example-01 ~]#
```

2. Su qualsiasi nodo nel cluster modificare **`/etc/cluster/cluster.conf`**

3. Aggiornare l'attributo **`config_version`** aumentando il proprio valore (per esempio, modificandolo da **`config_version="2"`** a **`config_version="3">`**).

4. Salvare **`/etc/cluster/cluster.conf`**.

5. Convalidare il file aggiornato con lo schemda del cluster (**`cluster.rng`**) eseguendo il comando **`ccs_config_validate`**. Per esempio:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

6. Se il file aggiornato è valido usare il comando **`scp`** per diffonderlo su **`/etc/cluster/`** in ogni nodo del cluster.

7. Verificare che il file di configurazione aggiornato è stato diffuso.

8. Su ogni nodo avviate il software del cluster consultando Sezione 8.1.1, «Avvio del software del cluster». Per esempio:

```
[root@example-01 ~]# service cman start
Starting cluster:
```

```
   Checking Network Manager...                                [  OK
]
   Global setup...                                            [  OK
]
   Loading kernel modules...                                  [  OK
]
   Mounting configfs...                                       [  OK
]
   Starting cman...                                           [  OK
]
   Waiting for quorum...                                      [  OK
]
   Starting fenced...                                         [  OK
]
   Starting dlm_controld...                                   [  OK
]
   Starting gfs_controld...                                   [  OK
]
   Unfencing self...                                          [  OK
]
   Joining fence domain...                                    [  OK
]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                               [  OK
]
Activating VG(s):   2 logical volume(s) in volume group "vg_example"
now active
                                                              [  OK
]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                         [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                         [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                             [  OK  ]
[root@example-01 ~]#
```

9. Su ogni nodo del cluster eseguire **cman_tool nodes** per verificare che i nodi siano membri attivi del cluster (contrassegnati con "M" nella colonna dello stato, "Sts"). Per esempio:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

10. Su qualsiasi nodo, utilizzando l'utilità **clustat**, verificate che i servizi HA siano in esecuzione come previsto. In aggiunta **clustat** mostra lo stato dei nodi del cluster. Per esempio:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
```

```
 node-02.example.com                          2 Online, rgmanager
 node-01.example.com                          1 Online, Local,
rgmanager

 Service Name                   Owner (Last)
State
 ------- ----                   ----- ------                    --
---
 service:example_apache         node-01.example.com
started
 service:example_apache2        (none)
disabled
```

11. Se il cluster è in esecuzione come previsto l'aggiornamento della configurazione è completato.

CAPITOLO 9. DIAGNOSI E CORREZIONE DEI PROBLEMI PRESENTI NEL CLUSTER

I problemi relativi al cluster sono per natura difficili da risolvere. Ciò è causato da un numero più elevato di sistemi rispetto alla diagnosi dei problemi per un singolo sistema. Tuttavia sono presenti problemi comuni che gli amministratori di sistema possono incontrare se implementano o amministrano un cluster. Sapere come affrontare questi problemi può facilitare l'implementazione e la gestione di un cluster.

Questo capitolo fornisce le informazioni relative ad alcuni cluster comuni sulle rispettive problematiche e sulla loro risoluzione. Per informazioni aggiuntive consultate il nostro knowledge base o contattate un rappresentante autorizzato di Red Hat. Se il vostro problema riguarda in modo particolare il file system GFS2, le informazioni relative alla risoluzione di problematiche comuni del GFS2 sono disponibili nel documento *Global File System 2*.

9.1. LE MODIFICHE ALLA CONFIGURAZIONE NON VENGONO IMPLEMENTATE

Se eseguite delle modifiche alla configurazione del cluster sarà necessario inoltrare le suddette modifiche su ogni nodo.

- Quando configurate un cluster usando **Conga**, esso sarà in grado di inoltrare automaticamente le modifiche al momento della loro implementazione.
- Per informazioni su come propagare le modifiche alla configurazione del cluster con il comando **ccs** consultare Sezione 5.15, «Propagazione del file di configurazione ai nodi del cluster».
- Per informazioni su come propagare le modifiche alla configurazione del cluster con gli strumenti della linea di comando consultare Sezione 8.4, «Aggiornamento di una configurazione».

Se apportate una delle seguenti modifiche alla configurazione del cluster non sarà necessario riavviare il cluster per una loro implementazione dopo averle inoltrate.

- Rimozione di un nodo dalla configurazione del cluster—*ad eccezione* di quando il conteggio dei nodi risulta passare da un numero maggiore di nodi ad un cluster con due nodi.
- Aggiungere un nodo alla configurazione del cluster—*ad eccezione* di quando il conteggio dei nodi risulta passare da un cluster con due nodi ad un cluster con più nodi.
- Modifica delle impostazioni per la registrazione
- Aggiungere, modificare o cancellare i servizi HA o i componenti VM.
- Aggiungere, modificare o cancellare le risorse del cluster.
- Aggiungere, modificare o cancellare i domini di failover.

Se eseguite ulteriori modifiche alla configurazione di un cluster sarà necessario riavviare il cluster stesso per una loro implementazione. Riavviare il cluster per implementare le seguenti modifiche:

- Aaggiungere o rimuovere l'opzione **two_node** dal file di configurazione del cluster.
- Modifica del nome del cluster.
- Modifica di qualsiasi timer **corosync** o **openais**.

- Aggiungere, modificare o cancellare gli euristici per il quorum disk, modifica di qualsiasi timer del quorum disk o del dispositivo relativo. Per l'implementazione di queste modifiche sarà necessario riavviare globalmente il demone **qdiskd**.
- Modifica della modalità **central_processing** per **rgmanager**. Per implementare questa modifica riavviare **rgmanager**.
- Modifica dell'indirizzo multicast.
- Smistamento della modalità di trasporto da UDP multicast a UDP unicast, o da UDP unicast a UDP multicast.

È possibile riavviare il cluster usando **Conga**, il comando **ccs**, o gli strumenti della linea di comando,

- Per informazioni sul riavvio di un cluster con **Conga** consultare Sezione 4.4, «Avvio, arresto, rimozione e riavvio del cluster».
- Per informazioni sul riavvio di un cluster con il comando **ccs** consultare Sezione 6.2, «Avvio ed arresto di un cluster».
- Per informazioni sul riavvio di un cluster con gli strumenti della linea di comando consultare Sezione 8.1, «Avvio ed arresto del software del cluster».

9.2. IMPOSSIBILE FORMARE IL CLUSTER

Se avete problemi nel formare un nuovo cluster controllate quanto di seguito riportato:

- Assicuratevi di aver impostato correttamente la risoluzione dei nomi. Il nome del nodo nel file **cluster.conf** deve corrispondere al nome usato per risolvere l'indirizzo del cluster attraverso la rete usata per le comunicazioni del cluster. Per esempio, se i nomi dei nodi del cluster risultano essere **nodea** e **nodeb** assicuratevi che entrambi i nodi contengano le voci corripsondenti nel file **/etc/cluster/cluster.conf** e **/etc/hosts**.
- Se il cluster utilizza multicast per le comunicazioni tra nodi assicuratevi che il traffico multicast non sia stato bloccato, che non vi sia alcun ritardo o che interferisca con un'altra rete usata dal cluster per le comunicazioni. Da notare che alcuni interruttori Cisco hanno alcune funzioni in grado di causare ritardi nel traffico multicast.
- Utilizzare **telnet** o **SSH** per verificare se è possibile raggiungere i nodi remoti.
- Eseguire il comando **ethtool eth1 | grep link** per controllare se il link ethernet è abilitato.
- Usare **tcpdump** su ogni nodo per controllare il traffico della rete.
- Assicuratevi che le regole del firewall non blocchino le comunicazioni tra i nodi.
- Assicuratevi che le interfacce usate dal cluster per le comunicazioni tra i nodi, non utilizzino modalità di bonding diverse da 0, 1 o 2. (Con Red Hat Enterprise Linux 6.4. le modalità 0 e 2 sono ora supportate).

9.3. IMPOSSIBILE UNIRE I NODI AL CLUSTER DOPO UN FENCING O UN RIAVVIO

Se i nodi non sono in grado di unirsi ad un cluster dopo un processo di fencing o di riavvio controllate quanto di seguito riportato:

- I cluster che utilizzano un interruttore Cisco Catalyst per passare il proprio traffico possono avere questo tipo di problema.
- Assicuratevi che tutti i nodi del cluster siano in possesso della stessa versione del file **cluster.conf**. Se il file **cluster.conf** è diverso in qualsiasi nodo, i nodi non saranno in grado di unirsi al cluster dopo un processo di fencing.

  Con Red Hat Enterprise Linux 6.1 sarà possibile utilizzare il seguente comando per verificare che tutti i nodi specificati nel file di configurazione del cluster dell'host siano in possesso di un file di configurazione identico.

  ```
  ccs -h host --checkconf
  ```

  Per informazioni sul comando **ccs** consultare Capitolo 5, *Configurazione di Red Hat High Availability Add-On con il comando **ccs*** e Capitolo 6, *Gestione di Red Hat High Availability Add-On con **ccs***.
- Assicuratevi di aver configurato **chkconfig on** per i servizi del cluster all'interno del nodo che stà cercando di unirsi al cluster.
- Assicuratevi che nessuna regola del firewall stia bloccando le comunicazioni del nodo con altri nodi del cluster.

9.4. ARRESTI INASPETTATI DEL DEMONE DEL CLUSTER

RGManager presenta un processo watchdog in grado di riavviare l'host se il processo **rgmanager** principale fallisce inaspettatamente. Tale processo causa l'isolamento del nodo, così facendo **rgmanager** sarà in grado di ripristinare il servizio su un altro host. Quando il demone watchdog rileva l'arresto inaspettato del processo **rgmanager**, esso eseguirà il riavvio del nodo. A tal punto il nodo isolato verrà rilevato ed espulso dai nodi attivi del cluster.

Il numero più basso di *process ID* (PID) rappresenta il processo watchdog che si verifica se il processo figlio relativo (il processo con un PID più elevato) si arresta inaspettatamente. La cattura del processo con un PID più elevato usando **gcore** può aiutarvi nel processo di troubleshooting di un demone.

Installare i pacchetti necessari per catturare e visualizzare il core ed assicurarsi che sia il **rgmanager** che **rgmanager-debuginfo** abbiano la stessa versione, in caso contrario il core dell'applicazione catturata potrebbe risultare instabile.

```
$ yum -y --enablerepo=rhel-debuginfo install gdb rgmanager-debuginfo
```

9.4.1. Cattura di rgmanager Core durante l'esecuzione

Durante l'esecuzione sono presenti due processi **rgmanager**. Sarà necessario catturare il core per il processo **rgmanager** con il PID più alto.

Di seguito viene riportato un output d'esempio del comando **ps** il quale mostra due processi per **rgmanager**.

```
$ ps aux | grep rgmanager | grep -v grep
```

```
root     22482  0.0  0.5  23544  5136 ?        S<Ls Dec01   0:00 rgmanager
root     22483  0.0  0.2  78372  2060 ?        S<l  Dec01   0:47 rgmanager
```

Nel seguente esempio il programma **pidof** determina automaticamente il pid con il numero più alto il quale rappresenta il pid appropriato per creare il core. Il comando completo cattura il core dell'applicazione per il processo 22483 con il numero più alto di PID.

```
$ gcore -o /tmp/rgmanager-$(date '+%F_%s').core $(pidof -s rgmanager)
```

9.4.2. Cattura del core durante l'arresto inaspettato del demone

Per impostazione predefinita lo script **/etc/init.d/functions** blocca i file principali dei demoni invocati tramite **/etc/init.d/rgmanager**. Per la creazione del core da parte di un demone sarà necessario abilitare l'opzione necessaria. Questa procedura deve essere eseguita su tutti inodi del cluster che necessitano di una cattura del core dell'applicazione.

Per creare un file principale in presenza di un crash del demone rgmanager modificare il file **/etc/sysconfig/cluster**. Il parametro ***DAEMONCOREFILELIMIT*** permette al demone di creare i file se il processo si arresta inaspettatamente. L'opzione **-w** impedisce al processo watchdog di essere eseguito. Il demone watchdog è responsabile per il riavvio dei nodi del cluster se si verifica un crash di **rgmanager**, e in alcuni casi, se il demone watchdog è in esecuzione il file principale non verrà generato, per questo motivo è necessario disabilitarlo.

```
DAEMONCOREFILELIMIT="unlimited"
RGMGR_OPTS="-w"
```

Riavvio di rgmanager per l'attivazione delle nuove opzioni di configurazione:

```
service rgmanager restart
```

NOTA

Se i servizi del cluster sono in esecuzione su questo nodo, i servizi stessi potrebbero essere in esecuzione con uno stato incorretto.

Il file core verrà salvato quando sarà generato da un arresto inaspettato del processo **rgmanager**.

```
ls /core*
```

L'output dovrebbe essere simile al seguente:

```
/core.11926
```

Spostare o cancellare qualsiasi file core vecchi nella directory / prima di riavviare **rgmanager** per poter catturare il core dell'applicazione. Riavviare o isolare il nodo sul quale si è verificato un arresto inaspettato di **rgmanager** dopo la cattura del core per assicurare che il processo watchdog non sia in esecuzione.

9.4.3. Registrazione di una sessisione di backtrace **gdb**

Dopo aver catturato il file core sarà possibile visualizzare il proprio contenuto usando **gdb**, GNU Debugger. Per registrare una sessione dello script di **gdb** sul file core del sistema interessato eseguire quanto di seguito riportato:

```
$ script /tmp/gdb-rgmanager.txt
$ gdb /usr/sbin/rgmanager /tmp/rgmanager-.core.
```

Così facendo verrà avviata una sessione **gdb**, mentre il comando **script** esegue la registrazione sul file di testo appropriato. Eseguire i seguenti comandi in **gdb**:

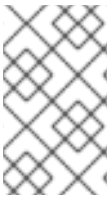
```
(gdb) thread apply all bt full
(gdb) quit
```

Premere **ctrl-D** per arrestare la sessione dello script e salvarla sul file di testo.

9.5. I SERVIZI DEL CLUSTER ENTRANO IN UNO STATO DI SOSPENSIONE

Quando i servizi del cluster cercano di eseguire l'isolamento di un nodo essi vengono arrestati fino al completamento dell'operazione di fencing. Per questo motivo se lo storage controllato dal cluster o i servizi entrano in uno stato di sospensione, ed i nodi del cluster mostrano una visuale diversa del membership del cluster, oppure se il cluster è sospeso quando cercate di isolare un nodo e sarà necessario riavviare i nodi per un ripristino, controllate quanto di seguito indicato:

- Il cluster avrà cercato di isolare un nodo ma tale operazione è fallita.
- Controllate il file **/var/log/messages** su tutti i nodi e verificate se sono presenti alcuni messaggi relativi al fallimento del fencing. In caso affermativo riavviare i nodi nel cluster e configurare correttamente il processo di fencing.
- Verificate che non sia presente alcuna partizione della rete, come riportato in Sezione 9.8, «Ogni nodo in un cluster a due nodi riporta l'arresto del secondo nodo», che sia possibile una comunicazione tra i nodi e la corretta esecuzione della rete.
- Se i nodi abbandonano il cluster i nodi restanti non avranno più il quorum corretto. Il cluster avrà bosogno del quorum corretto per operare. Con la rimozione dei nodi il cluster non avrà più il quorum necessario per i servizi e si verificherà una sospensione dello storage e dei servizi stessi. In tal caso modificare i voti previsti o implementate nuovamente il numero di nodi all'interno del cluster.



NOTA

È possibile isolare un nodo manualmente con il comando **fence_node** o utilizzando **Conga**. Per informazioni consultare la pagina man di **fence_node** e Sezione 4.3.2, «Esclusione o inserimento di un nodo nel cluster».

9.6. IL SERVIZIO DEL CLUSTER NON SI AVVIA

Se un servizio controllato dal cluster non si avvia controllare quanto di seguito riportato.

- Potrebbe essere presente un errore di sintassi nella configurazione del servizio in **cluster.conf**. Utilizzare il comando **rg_test** per convalidare la sintassi nella configurazione. Se sono presenti alcuni errori nella sintassi o nella configurazione il comando **rg_test** sarà in

grado di notificarvelo.

```
$ rg_test test /etc/cluster/cluster.conf start service servicename
```

Per maggiori informazioni sul comando **rg_test** consultate Sezione C.5, «Servizi di debug e di prova ed ordine delle risorse».

Se la configurazione è valida allora aumentate il login del gestore del gruppo di risorse e consultate i log dei messaggi per determinare la causa del fallimento dell'avvio del servizio. È possibile aumentare il livello dei log aggiungendo il parametro **loglevel="7"** sul tag **rm** nel file **cluster.conf**. Così facendo aumenterete la verbosità dei messaggi in relazione all'avvio, arresto e migrazione dei servizi clusterizzati.

9.7. I SERVIZI CONTROLLATI DAL CLUSTER NON ESEGUONO LA MIGRAZIONE

Se un servizio controllato dal cluster non esegue la migrazione su un altro nodo ma il servizio esegue l'avvio su un nodo specifico controllare quanto di seguito riportato.

- Assicuratevi che le risorse necessarie all'esecuzione del servizio siano presenti su tutti i nodi nel cluster che devono eseguire il servizio in questione. Per esempio, se il servizio clusterizzato assume un file di script in una posizione specifica o un file system montato su di un mount point, allora assicuratevi che le risorse siano disponibili nelle posizioni previste su tutti i nodi del cluster.
- Assicuratevi che i domini di failover, le dipendenze dei servizi e la loro esclusività non siano configurati in modo da impedire la migrazione in modo previsto dei servizi.
- Se il servizio in questione è una risorsa della macchina virtuale controllate la documentazione in modo da assicurare che tutte le impostazioni corrette della configurazione siano state completate.
- Aumentate il login del gestore del gruppo di risorse come descritto in Sezione 9.6, «Il servizio del cluster non si avvia» e successivamente leggere i log dei messaggi per determinare la causa del fallimento della migrazione del servizio.

9.8. OGNI NODO IN UN CLUSTER A DUE NODI RIPORTA L'ARRESTO DEL SECONDO NODO

Se il cluster è composto da due nodi ed ogni nodo riporta il normale funzionamento ma al tempo stesso riporta che il secondo nodo non è in funzione, ciò indicherà che i nodi non sono in grado di comunicare tra loro tramite multicast attraverso il cluster heartbeat network. Conosciuto anche come "split brain" o "network partition." Per risolvere questo problema controllate le condizioni riportate in Sezione 9.2, «Impossibile formare il cluster».

9.9. I NODI SONO ISOLATI IN PRESENZA DI UN ERRORE DEL PERCORSO LUN

Se un nodo viene isolato ogni qualvolta si verifica un fallimento del percorso LUN ciò potrebbe essere causato dall'uso di un quorum disk attraverso uno storage di tipo multipath. Se utilizzate un quorum disk attraverso uno storage di tipo multipath assicuratevi di avere tutte le impostazioni corrette per tollerare un fallimento del percorso.

9.10. IL QUORUM DISK NON APPARE COME MEMBRO DEL CLUSTER

Se avete configurato il sistema all'uso di un quorum disk ma lo stesso non appare come membro del cluster controllate quanto di seguito riportato.

- Assicuratevi di aver impostato **`chkconfig on`** per il servizio **`qdisk`**.
- Assicuratevi di aver iniziato il servizio **`qdisk`**.
- Da notare che potranno essere necessari alcuni minuti per la registrazione del quorum disk con il cluster. Questo è un comportamento normale e previsto.

9.11. COMPORTAMENTO NON PREVISTO DEL PROCESSO DI FAILOVER

Un problema comune con i server del cluster è il comportamento non previsto del processo di failover. Alcuni servizi verranno arrestati all'avvio di altri o alcuni di essi non eseguiranno il riavvio al verificarsi del failover. Tale comportamento si può verificare se sono implementati sistemi complessi di failover i quali consistono in domini di failover e dipendenze ed esclusività dei servizi. Per risolvere questo problema provate ad implementare un servizio o una configurazione del dominio di failover più semplice. Evitare le funzioni di esclusività e di dipendenza del servizio se non siete a conoscenza di come queste funzioni possono interessare il failover in qualsiasi condizione.

9.12. IL PROCESSO DI FENCING SI VERIFICA RANDOMICAMENTE

Se un nodo è stato isolato randomicamente controllate quanto di seguito riportato.

- Questo tipo di comportamento si verifica *sempre* a causa di una perdita del token da parte di un nodo con una conseguente perdita di qualsiasi contatto con il resto del cluster e di una assenza di qualsiasi heartbeat.
- Qualsiasi situazione in cui si verifica una assenza di heartbeat da parte del sistema all'interno di un intervallo specificato dal token può causare un processo di fencing. Per impostazione predefinita l'intervallo specificato è di 10 secondi. Esso può essere variato aggiungendo il valore desiderato (in millisecondi) nel parametro del token del tag relativo al totem nel file di configurazione **`cluster.conf`** (per esempio impostando **`totem token="30000"`** su 30 secondi).
- Assicuratevi che la rete stia funzionando come previsto.
- Assicuratevi che le interfacce usate dal cluster per le comunicazioni tra i nodi, non utilizzino modalità di bonding diverse da 0, 1 o 2. (Con Red Hat Enterprise Linux 6.4. le modalità 0 e 2 sono ora supportate).
- Cercate di determinare se il sistema è "freezing" 'sospeso' o se in presenza di un kernel panic. Impostate l'utilità **`kdump`** e controllate se riuscite ad ottenere un core durante una di queste fasi.
- Assicuratevi che non vi siano altri motivi a causa dei quali attribuire erroneamente un fencing, per esempio se si verifica una espulsione da parte del quorum disk di un nodo a causa di un fallimento dello storage oppure in presenza di un prodotto di terzi, come Oracle RAC, il quale esegue il riavvio del nodo a causa di condizioni esterne. I log dei messaggi sono spesso molto utili nel determinare questo tipo di problemi. Ogni qualvolta si verifica l'isolamento di un nodo o un suo riavvio, consultare sempre i log dei messaggi di tutti i nodi presenti nel cluster.

- Controllate l'intero sistema per la presenza di errori hardware che possono causare l'impossibilità da parte di un sistema di rispondere agli heartbeat come previsto.

9.13. LA REGISTRAZIONE DEL DEBUG PER IL DISTRIBUTED LOCK MANAGER (DLM) DEVE ESSERE ABILITATA

Se necessario è possibile abilitare due opzioni di debug per il Distributed Lock Manager (DLM): DLM kernel debugging e POSIX lock debugging.

Per abilitare il DLM debugging, modificare il file **/etc/cluster/cluster.conf** in modo da poter aggiungere le opzioni al tag **dlm**. L'opzione **log_debug** abilita i messaggi per il DLM kernel debugging mentre l'opzione **plock_debug** abilita i messaggi per il POSIX lock debugging.

Il seguente esempio mostra una sezione di un file \n**/etc/cluster/cluster.conf** con il tag **dlm** il quale abilita entrambe le opzioni di debug DLM:

```
<cluster config_version="42" name="cluster1">
  ...
  <dlm log_debug="1" plock_debug="1"/>
  ...
</cluster>
```

Dopo la modifica di **/etc/cluster/cluster.conf** eseguire il comando **cman_tool version -r** per propagare la configurazione al resto dei nodi del cluster.

CAPITOLO 10. CONFIGURAZIONE SNMP CON RED HAT HIGH AVAILABILITY ADD-ON

Con Red Hat Enterprise Linux 6.1 e versioni più recenti il Red Hat High Availability Add-On fornisce il supporto per le Trap SNMP. Questo capitolo descrive il metodo attraverso il quale configurare il sistema per SNMP, seguito da un sommario relativo alle Trap emesse da Red Hat High Availability Add-On per determinati eventi del cluster.

10.1. SNMP E RED HAT HIGH AVAILABILITY ADD-ON

L'agente SNMP di Red Hat High Availability Add-On è **foghorn**, esso emette le Trap SNMP. L'agente **foghorn** comunica con il demone **snmpd** per mezzo del protocollo AgentX. Il suddetto agente crea solo le Trap SNMP; non supporta altre operazioni SNMP come ad esempio **get** o **set**.

Attualmente non sono disponibili opzioni **config** per l'agente **foghorn**. Esso non può essere configurato all'uso di un socket specifico; è supportato solo il socket AgentX predefinito.

10.2. CONFIGURAZIONE DI SNMP CON IL RED HAT HIGH AVAILABILITY ADD-ON

Per configurare SNMP con il Red Hat High Availability Add-On eseguire le seguenti fasi su ogni nodo nel cluster per assicurarsi che i servizi necessari siano abilitati ed in esecuzione.

1. Per usare SNMP traps con Red Hat High Availability Add-On è necessario utilizzare il servizio **snmpd** come master agent. Poichè **foghorn** è un agente secondario ed utilizza il protocollo AgentX sarà necessario aggiungere la seguente riga al file **/etc/snmp/snmpd.conf** per abilitare il supporto AgentX:

   ```
   master agentx
   ```

2. Per specificare l'host al quale inviare le notifiche Trap SNMP aggiungere la seguente riga al file **/etc/snmp/snmpd.conf**:

   ```
   trap2sink host
   ```

   Per maggiori informazioni sulla gestione delle notifiche consultare la pagina man di **snmpd.conf**.

3. Assicuratevi che il demone **snmpd** sia stato abilitato ed è in esecuzione tramite i seguenti comandi:

   ```
   # chkconfig snmpd on
   # service snmpd start
   ```

4. Se il demone **messagebus** non è stato abilitato e non è in esecuzione eseguire i seguenti comandi:

   ```
   # chkconfig messagebus on
   # service messagebus start
   ```

5. Assicuratevi che il demone **foghorn** sia stato abilitato ed è in esecuzione tramite i seguenti comandi:

```
# chkconfig foghorn on
# service foghorn start
```

6. Eseguire il seguente comando per configurare il sistema in modo tale che **COROSYNC-MIB** sia in grado di generare le Trap SNMP, e per assicurare che il demone **corosync-notifyd** sia abilitato ed in esecuzione:

```
# echo "OPTIONS=\"-d\" " > /etc/sysconfig/corosync-notifyd
# chkconfig corosync-notifyd on
# service corosync-notifyd start
```

Dopo aver configurato ogni nodo nel cluster per SNMP ed assicurato che i servizi necessari siano in esecuzione, i segnali D-bus saranno ricevuti dal servizio **foghorn** e tradotti in Trap SNMPv2. Le suddette Trap verranno passate all'host da voi definito con la voce **trapsink** per la ricezione di Trap SNMPv2.

10.3. INOLTRO DI TRAP SNMP

È possibile inoltrare Trap SNMP ad una macchina esterna al cluster dove sarà possibile utilizzare il demone **snmptrapd** sulla macchina esterna e personalizzare il metodo di risposta per le notifiche.

Per inoltrare le Trap SNMP su una macchina che non fa parte dei nodi del cluster eseguire le seguenti fasi:

1. Per ogni nodo del cluster seguire la procedura descritta in Sezione 10.2, «Configurazione di SNMP con il Red Hat High Availability Add-On», impostare la voce **trap2sink *host*** nel file **/etc/snmp/snmpd.conf** in modo da specificare l'host esterno che eseguirà il demone **snmptrapd**.

2. Sull'host esterno che riceverà le Trap modificare il file di configurazione **/etc/snmp/snmptrapd.conf** per specificare le stringhe della community. Per esempio, usare la seguente voce per permettere al demone **snmptrapd** di processare le notifiche usando la stringa della community **public**.

```
authCommunity log,execute,net public
```

3. Sull'host esterno che riceverà le Trap assicuratevi che il demone **snmptrapd** sia abilitato e in esecuzione eseguendo i seguenti comandi:

```
# chkconfig snmptrapd on
# service snmptrapd start
```

Per maggiori informazioni sulla processazione delle notifiche SNMP consultare la pagina man **snmptrapd.conf**.

10.4. TRAP SNMP CREATE DA RED HAT HIGH AVAILABILITY ADD-ON

Il demone **foghorn** genera le seguenti trap:

- **fenceNotifyFenceNode**

  La suddetta Trap si verifica quando un nodo isolato cerca di isolare un altro nodo. Da notare che questa trap viene generata su un nodo -- il nodo che ha tentato di eseguire l'operazione di fencing. La notifica include i seguenti campi:

  - **fenceNodeName** - nome del nodo isolato
  - **fenceNodeID** - id del nodo isolato
  - **fenceResult** - il risultato dell'operazione di fencing (0 per un successo, -1 se si verifica un errore, -2 se non si definisce alcun metodo di fencing)

- **rgmanagerServiceStateChange**

  Questa trap si verifica quando lo stato di un servizio del cluster è stato modificato. La notifica include i seguenti campi:

  - **rgmanagerServiceName** - il nome del servizio, che include il tipo di servizio (per esempio, **service:foo** o **vm:foo**).
  - **rgmanagerServiceState** - lo stato del servizio. Esclude gli stati di transizione come ad esempio **starting** e **stopping** per ridurre il disordine nelle trap.
  - **rgmanagerServiceFlags** - i flag del servizio. Sono attualmente presenti due flag supportati: **frozen**, il quale indica un servizio che è stato sospeso utilizzando **clusvcadm -Z**, e **partial**, il quale indica un servizio nel quale una risorsa fallita è stata riportata come **non-critical**, in questo caso la risorsa può fallire ed i suoi componenti possono essere riavviati manualmente senza interessare l'intero servizio.
  - **rgmanagerServiceCurrentOwner** - il proprietario del servizio. Se il servizio non è in esecuzione esso sarà **(none)**.
  - **rgmanagerServicePreviousOwner** - l'ultimo proprietario del servizio, seconosciuto. Se l'ultimo proprietario non è conosciuto esso potrà indicare **(none)**.

Il demone **corosync-nodifyd** genera le seguenti trap:

- **corosyncNoticesNodeStatus**

  Questa trap si verifica quando un nodo si unisce o abbandona il cluster. La notifica include i seguenti campi:

  - **corosyncObjectsNodeName** - nome del nodo
  - **corosyncObjectsNodeID** - id del nodo
  - **corosyncObjectsNodeAddress** - indirizzo IP del nodo
  - **corosyncObjectsNodeStatus** - stato del nodo (**joined** o **left**)

- **corosyncNoticesQuorumStatus**

  Questa trap si verifica quando lo stato del quorum varia. La notifica include i seguenti campi:

  - **corosyncObjectsNodeName** - nome del nodo

- **corosyncObjectsNodeID** - id del nodo
- **corosyncObjectsQuorumStatus** - nuovo stato del quorum (**quorate** o **NOT quorate**)

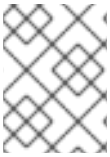
- **corosyncNoticesAppStatus**

  Questa trap si verifica quando una applicazione client si collega o scollega da Corosync.

  - **corosyncObjectsNodeName** - nome del nodo
  - **corosyncObjectsNodeID** - id del nodo
  - **corosyncObjectsAppName** - nome applicazione
  - **corosyncObjectsAppStatus** - nuovo stato dell'applicazione (**connected** o **disconnected**)

CAPITOLO 11. CONFIGURAZIONE SAMBA CLUSTERIZZATO

Con Red Hat Enterprise Linux 6.2 Red Hat High Availability Add-On fornisce un supporto per Samba clusterizzati in esecuzione con una configurazione attiva/attiva. Per fare questo installare e configurare CTDB su tutti i nodi presenti in un cluster usati insieme ai file system GFS2 clusterizzati.



NOTA

Red Hat Enterprise Linux 6 supporta Samba clusterizzati con un massimo di quattro nodi in esecuzione.

Questo capitolo descrive la procedura per la configurazione di CTDB attraverso la configurazione di un sistema di esempio. Per informazioni su come configurare i file system GFS2 consultare il *Global File System 2*. Per informazioni su come configurare i volumi logici consultare il *Logical Volume Manager Administration*.

11.1. PANORAMICA DI CTDB

CTDB è una implementazione cluster del database TDB usata da Samba. Per usare CTDB è necessario avere un file system clusterizzato condiviso su tutti i nodi presenti nel cluster. CTDB fornisce funzioni clusterizzate insieme al file system clusterizzato. Con Red Hat Enterprise Linux 6.2, CTDB esegue anche un cluster stack in parallelo a quello fornito dal clustering di Red Hat Enterprise Linux. CTDB gestisce l'appartenenza dei nodi, il ripristino/failover, il riposizionamento dell'IP ed i servizi di Samba.

11.2. PACCHETTI NECESSARI

Insieme ai pacchetti standard necessari per eseguire Red Hat High Availability Add-On e Red Hat Resilient Storage Add-On, l'esecuzione di Samba con il clustering di Red Hat Enterprise Linux ha bisogno dei seguenti pacchetti:

- **`ctdb`**
- **`samba`**
- **`samba-common`**
- **`samba-winbind-clients`**

11.3. CONFIGURAZION GFS2

La configurazione di Samba con Red Hat Enterprise Linux clustering richiede l'utilizzo di due file system GFS2: Un file system piccolo per CTDB ed un secondo file system per la condivisione di Samba. Questo esempio mostra come creare i due file system GFS2.

Prima di creare i file system GFS2 creare un volume logico LVM per ogni file system. Per informazioni su come creare i volumi logici LVM consultare il *Logical Volume Manager Administration*. In questo esempio vengono utilizzati i seguenti volumi logici:

- **`/dev/csmb_vg/csmb_lv`**, il quale conterrà i dati dell'utente da esportare tramite una condivisione Samba con una dimensione idonea. In questo esempio è stato creato un volume logico con una dimensione di 100GB.

- **/dev/csmb_vg/ctdb_lv**, che conterrà le informazioni condivise relative allo stato CTDB con una dimensione di 1GB.

Create gruppi di volumi clusterizzati e volumi logici solo su un nodo del cluster.

Per creare un file system GFS2 su un volume logico eseguire il comando **mkfs.gfs2**. Eseguire il suddetto comando solo su un nodo del cluster.

Per creare il file system ed ospitare la condivisione di Samba sul volume logico **/dev/csmb_vg/csmb_lv**, eseguire il seguente comando:

```
[root@clusmb-01 ~]# mkfs.gfs2 -j3 -p lock_dlm -t csmb:gfs2
/dev/csmb_vg/csmb_lv
```

Di seguito viene riportato il significato dei parametri:

-j

Specifica il numero di journal da creare nel file system. Questo esempio utilizza un cluster con tre nodi, per questo motivo possiamo creare un journal per nodo.

-p

Specifica il protocollo di blocco. **lock_dlm** è il protocollo di blocco usato da GFS2 per una comunicazione tra i nodi.

-t

Specifica il nome di lock table con un formato *cluster_name:fs_name*. In questo esempio il nome del cluster specificato nel file **cluster.conf** è **csmb**, e **gfs2** verrà utilizzato come nome del file system.

L'output di questo comando è il seguente:

```
This will destroy any data on /dev/csmb_vg/csmb_lv.
  It appears to contain a gfs2 filesystem.

Are you sure you want to proceed? [y/n] y

Device:
/dev/csmb_vg/csmb_lv
Blocksize:  4096
Device Size  100.00 GB (26214400 blocks)
Filesystem Size: 100.00 GB (26214398 blocks)
Journals:  3
Resource Groups:  400
Locking Protocol:   "lock_dlm"
Lock Table:   "csmb:gfs2"
UUID:
  94297529-ABG3-7285-4B19-182F4F2DF2D7
```

In questo esempio il file system **/dev/csmb_vg/csmb_lv** verrà montato su **/mnt/gfs2** in tutti i nodi. Questo mount point deve corrispondere al valore specificato come posizione della directory **share** con l'opzione **path =** nel file **/etc/samba/smb.conf**, come descritto in Sezione 11.5, «Configurazione di Samba».

Per creare il file system ed ospitare le informazioni sullo stato di CTDB sul volume logico **/dev/csmb_vg/csmb_lv**, eseguire il seguente comando:

```
[root@clusmb-01 ~]# mkfs.gfs2 -j3 -p lock_dlm -t csmb:ctdb_state
/dev/csmb_vg/ctdb_lv
```

Da notare che questo comando specifica un nome per il lock table diverso rispetto a quello dell'esempio nel quale è stato creato il file system su **/dev/csmb_vg/csmb_lv**. Così facendo verrà eseguita una distinzione tra i nomi dei lock table per i diversi dispositivi usati per i file system.

L'output di **mkfs.gfs2** è il seguente:

```
This will destroy any data on /dev/csmb_vg/ctdb_lv.
  It appears to contain a gfs2 filesystem.

Are you sure you want to proceed? [y/n] y

Device:
/dev/csmb_vg/ctdb_lv
Blocksize:    4096
Device Size   1.00 GB (262144 blocks)
Filesystem Size:  1.00 GB (262142 blocks)
Journals:  3
Resource Groups:  4
Locking Protocol:  "lock_dlm"
Lock Table:   "csmb:ctdb_state"
UUID:
  BCDA8025-CAF3-85BB-B062-CC0AB8849A03
```

In questo esempio il file system **/dev/csmb_vg/ctdb_lv** verrà montato su **/mnt/ctdb** su tutti i nodi. Il mount point deve corrispondere al valore specificato come posizione del file **.ctdb.lock** con l'opzione **CTDB_RECOVERY_LOCK** nel file **/etc/sysconfig/ctdb** come descritto in Sezione 11.4, «Configurazione di CTDB».

11.4. CONFIGURAZIONE DI CTDB

Il file di configurazione CTDB si trova in **/etc/sysconfig/ctdb**. I campi obbligatori da configurare per l'operazione CTDB sono i seguenti:

- **CTDB_NODES**
- **CTDB_PUBLIC_ADDRESSES**
- **CTDB_RECOVERY_LOCK**
- **CTDB_MANAGES_SAMBA** (deve essere abilitato)
- **CTDB_MANAGES_WINBIND** (deve essere abilitato se in esecuzione su un server membro)

I seguenti esempi mostrano un file di configurazione con i campi obbligatori per l'operazione CTDB impostati con parametri d'esempio.

```
CTDB_NODES=/etc/ctdb/nodes
CTDB_PUBLIC_ADDRESSES=/etc/ctdb/public_addresses
```

```
CTDB_RECOVERY_LOCK="/mnt/ctdb/.ctdb.lock"
CTDB_MANAGES_SAMBA=yes
CTDB_MANAGES_WINBIND=yes
```

Di seguito viene riportato il significato dei parametri:

CTDB_NODES

Specifica la posizione del file che contiene l'elenco dei nodi del cluster.

Il file **/etc/ctdb/nodes** indicato da **CTDB_NODES** elenca gli indirizzi IP dei nodi del cluster, come riportato nel seguente esempio:

```
192.168.1.151
192.168.1.152
192.168.1.153
```

In questo esempio è presente solo una interfaccia/IP su ogni nodo per le comunicazioni cluster/CTDB e per i client. Tuttavia è fortemente consigliato che ogni nodo del cluster sia in possesso di due interfacce, in questo modo un set di interfacce può essere usato per le comunicazioni cluster/CTDB, ed un altro per l'accesso del client pubblico. Usare gli indirizzi IP appropriati della rete del cluster ed assicurarsi che gli indirizzi IP/hostname usati nel file **cluster.conf** siano gli stessi. In modo simile, usare le interfacce appropriate della rete pubblica per l'accesso client nel file **public_addresses**.

È importantissimo che il file **/etc/ctdb/nodes** sia identico su tutti i nodi poichè l'ordine è molto importante, per questo motivo CTDB fallisce se trova informazioni diverse sui nodi.

CTDB_PUBLIC_ADDRESSES

Specifica la posizione del file che elenca gli indirizzi IP utilizzabili per l'accesso alle condivisioni Samba esportate da questo cluster. Questi sono gli indirizzi IP da configurare in DNS per il nome del server di Samba clusterizzato, e rappresentano gli indirizzi usati dai client CIFS per il collegamento. Configurare il nome del server Samba clusterizzato come un record tipo A del DNS con indirizzi IP multipli ed usate una distribuzione round-robin DNS dei client su tutti i nodi del cluster.

Per questo esempio è stata configurata una voce round-robin DNS **csmb-server** con tutti gli indirizzi elencati nel file **/etc/ctdb/public_addresses**. Il DNS distribuirà i client che utilizzano questa voce sul cluster con una modalità round-robin.

I contenuti del file **/etc/ctdb/public_addresses** su ogni nodo sono i seguenti:

```
192.168.1.201/0 eth0
192.168.1.202/0 eth0
192.168.1.203/0 eth0
```

In questo esempio vengono utilizzati tre indirizzi non attualmente utilizzati sulla rete. Nella vostra configurazione usate indirizzi accessibili da parte dei client desiderati.

Alternativamente questo esempio mostra i contenuti dei file **/etc/ctdb/public_addresses** in un cluster, nel quale sono presenti tre nodi ma con un totale di quattro indirizzi pubblici. Qui l'indirizzo IP 198.162.2.1 può essere ospitato dal nodo 0 o nodo 1 e sarà disponibile ai client se uno di suddetti nodi risulta essere disponibile. Solo se i nodi 0 e 1 falliscono l'indirizzo pubblico non risulta essere più disponibile ai client. Tutti gli altri indirizzi pubblici possono essere serviti da un solo nodo e quindi disponibili se il nodo in questione è anch'esso disponibile.

Il file **/etc/ctdb/public_addresses** sul nodo 0 include i seguenti contenuti:

```
198.162.1.1/24 eth0
198.162.2.1/24 eth1
```

Il file **/etc/ctdb/public_addresses** sul nodo 1 include i seguenti contenuti:

```
198.162.2.1/24 eth1
198.162.3.1/24 eth2
```

Il file **/etc/ctdb/public_addresses** sul nodo 2 include i seguenti contenuti:

```
198.162.3.2/24 eth2
```

CTDB_RECOVERY_LOCK

Specifica un file di blocco usato internamente da CTDB per il ripristino. Questo file deve risiedere su uno storage condiviso e quindi deve essere accessibile da tutti i nodi presenti nel cluster. L'esempio in questa sezione utilizza il file system GFS2 che verrà montato su **/mnt/ctdb** su tutti i nodi. Questo è diverso dal file system GFS2 che conterrà la condivisione Samba da esportare. Questo file di blocco usato per il ripristino impedisce la possibilità di scenari split-brain. Con nuove versioni di CTDB (1.0.112 e versioni più recenti), è possibile specificare facoltativamente questo file se si specifica un meccanismo alternativo di prevenzione alla sindrome split-brain.

CTDB_MANAGES_SAMBA

Se abilitato ed impostato su **yes**, CTDB è in grado di avviare ed arrestare il servizio Samba se necessario, per eseguire una migrazione/failover del servizio.

Quando **CTDB_MANAGES_SAMBA** è abilitato è necessario disabilitare un avvio **init** automatico dei demoni **smb** e **nmb** eseguendo i seguenti comandi:

```
[root@clusmb-01 ~]# chkconfig snb off
[root@clusmb-01 ~]# chkconfig nmb off
```

CTDB_MANAGES_WINBIND

Se abilitato impostandolo su **yes**, CTDB è in grado di avviare ed arrestare il demone **winbind**. Abilitatelo quando utilizzate CTDB in un dominio Windows o in una modalità di sicurezza della directory attiva.

Quando **CTDB_MANAGES_SAMBA** è abilitato è necessario disabilitare un avvio **init** automatico del demone **winbind** eseguendo il seguente comando:

```
[root@clusmb-01 ~]# chkconfig windinbd off
```

11.5. CONFIGURAZIONE DI SAMBA

In questo esempio il file di configurazione di Samba **smb.conf** si trova in **/etc/samba/smb.conf**. Esso contiene i seguenti parametri:

```
[global]
```

```
 guest ok = yes
 clustering = yes
 netbios name = csmb-server
[csmb]
 comment = Clustered Samba
  public = yes
 path = /mnt/gfs2/share
 writeable = yes
 ea support = yes
```

In questo esempio viene esportata una condivisione **csmb** posizionata in **/mnt/gfs2/share**. Ciò è diverso da un file system condiviso GFS2 su **/mnt/ctdb/.ctdb.lock** specificato come parametro **CTDB_RECOVERY_LOCK** nel file di configurazione CTDB su **/etc/sysconfig/ctdb**.

In questo esempio verrà creata la directory **share** in **/mnt/gfs2** durante il primo montaggio. La voce **clustering = yes** indica a Samba di usare CTDB. La voce **netbios name = csmb-server** imposta esplicitamente tutti i nodi in modo da avere un nome NetBIOS comune. Il parametro **ea support** è necessario se desiderate usare gli attributi estesi.

Il file di configurazione **smb.conf** deve essere identico su tutti i nodi del cluster.

Samba offre anche una configurazione basata sulla registrazione tramite il comando **net conf**. Ciò permette di mantenere automaticamente la configurazione in sincronizzazione tra i membri del cluster, senza dover copiare manualmente i file di configurazione tra i nodi. Per informazioni sul comando **net conf**, consultare le pagine man di **net**(8).

11.6. AVVIO DI CTDB E DEI SERVIZI SAMBA

Dopo aver avviato il cluster sarà necessario montare i file system GFS2 creati come descritto in Sezione 11.3, «Configurazion GFS2». I permessi sulla directory **share** di Samba e gli account utente sui nodi del cluster, devono essere impostati per un accesso client.

Eseguire il seguente comando su tutti i nodi per avviare il demone **ctdbd**. Poichè in questo esempio CTDB è stato configurato con **CTDB_MANAGES_SAMBA=yes**, CTDB avvierà il servizio Samba su tutti i nodi ed esporterà tutte le condivisioni Samba configurate.

```
[root@clusmb-01 ~]# service ctdb start
```

Potrà essere necessario qualche minuto per avviare Samba, esportare le condivisioni e stabilizzare. L'esecuzione di **ctdb status** mostra lo stato di CTDB come nel seguente esempio:

```
[root@clusmb-01 ~]# ctdb status
Number of nodes:3
pnn:0 192.168.1.151     OK (THIS NODE)
pnn:1 192.168.1.152     OK
pnn:2 192.168.1.153     OK
Generation:1410259202
Size:3
hash:0 lmaster:0
hash:1 lmaster:1
hash:2 lmaster:2
Recovery mode:NORMAL (0)
Recovery master:0
```

Quando tutti i nodi sono "OK", sarà possibile usare in sicurezza il server Samba clusterizzato come descritto in Sezione 11.7, «Utilizzo del server Samba clusterizzato».

11.7. UTILIZZO DEL SERVER SAMBA CLUSTERIZZATO

I client potranno collegarsi alla condivisione esportata di Samba tramite il collegamento ad uno degli indirizzi IP specificati nel file **/etc/ctdb/public_addresses**, oppure usando la voce DNS **csmb-server** precedentemente configurata come di seguito riportato:

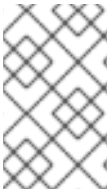
```
[root@clusmb-01 ~]# mount -t cifs //csmb-server/csmb /mnt/sambashare -o
user=testmonkey
```

o

```
[user@clusmb-01 ~]$ smbclient //csmb-server/csmb
```

APPENDICE A. PARAMETRI DEL DISPOSITIVO DI FENCING

La suddetta appendice fornisce le tabelle contenenti le descrizioni dei parametri dei dispositivi di fencing. È possibile configurare i parametri con **luci** utilizzando il comando **`ccs`** o modificando **`etc/cluster/cluster.conf`**. Per un elenco completo e descrizioni dei parametri del dispositivo di fencing per ogni fence agent consultare la pagina man corrispondente.



NOTA

Il parametro **Nome** per un dispositivo di fencing specifica un nome arbitrario per il dispositivo che sarà usato da Red Hat High Availability Add-On. Tale nome non sarà uguale al nome DNS per il dispositivo.

NOTA

Alcuni dispositivi per il fencing possiedono un parametro **Script Password** opzionale. Il parametro **Script Password** permette all'utente di specificare che la password per il dispositivo di fencing viene fornita tramite uno script e non tramite un parametro **Password**. L'uso di uno **Script Password** sostituisce il parametro **Password** rendendo così la password non visibile nel file di configurazione del cluster (**`/etc/cluster/cluster.conf`**).

Tabella A.1, «Sommario dei dispositivi di fencing» elenca i dispositivi di fencing, gli agenti dei dispositivi di fencing associati e fornisce un riferimento alla tabella di documentazione dei parametri per i dispositivi di fencing.

Tabella A.1. Sommario dei dispositivi di fencing

Dispositivo di fencing	Fence Agent	Riferimento alla descrizione del parametro
APC Power Switch (telnet/SSH)	fence_apc	Tabella A.2, «APC Power Switch (telnet/SSH)»
Brocade Fabric Switch	fence_brocade	Tabella A.4, «Brocade Fabric Switch»
Cisco MDS	fence_cisco_mds	Tabella A.5, «Cisco MDS»
Cisco UCS	fence_cisco_ucs	Tabella A.6, «Cisco UCS»
Dell DRAC 5	fence_drac5	Tabella A.7, «Dell DRAC 5»
Eaton Network Power Switch (Interfaccia SNMP)	fence_eaton_snmp	Tabella A.8, «Eaton Network Power Controller (Interfaccia SNMP) (Red Hat Enterprise Linux 6.4 e versioni più recenti)»
Controllore Egenera SAN	fence_egenera	Tabella A.9, «Controllore Egenera SAN»

Dispositivo di fencing	Fence Agent	Riferimento alla descrizione del parametro
ePowerSwitch	fence_eps	Tabella A.10, «ePowerSwitch»
Fence virt	fence_virt	Tabella A.11, «Fence virt»
Fujitsu Siemens Remoteview Service Board (RSB)	fence_rsb	Tabella A.12, «Fujitsu Siemens Remoteview Service Board (RSB)»
HP BladeSystem	fence_hpblade	Tabella A.13, «HP BladeSystem (Red Hat Enterprise Linux 6.4 e versioni più recenti)»
HP iLO/iLO2 (Integrated Lights Out)	fence_ilo	Tabella A.14, «HP iLO/iLO2 (Integrated Lights Out)»
HP iLO (Integrated Lights Out) MP	fence_ilo_mp	Tabella A.15, «HP iLO (Integrated Lights Out) MP»
IBM BladeCenter	fence_bladecenter	Tabella A.16, «IBM BladeCenter»
IBM BladeCenter SNMP	fence_ibmblade	Tabella A.17, «IBM BladeCenter SNMP»
IBM iPDU	fence_ipdu	Tabella A.18, «IBM iPDU (Red Hat Enterprise Linux 6.4 e versioni più recenti)»
IF MIB	fence_ifmib	Tabella A.19, «IF MIB»
Intel Modular	fence_intelmodular	Tabella A.20, «Intel Modular»
IPMI (Intelligent Platform Management Interface) LAN	fence_ipmilan	Tabella A.21, «IPMI (Intelligent Platform Management Interface) LAN»
RHEV-M REST API	fence_rhevm	Tabella A.22, «RHEV-M REST API (RHEL 6.2 e versione più recente, RHEV 3.0 e versione più recente)»

Dispositivo di fencing	Fence Agent	Riferimento alla descrizione del parametro
SCSI Fencing	fence_scsi	Tabella A.23, «SCSI Fencing»
VMware Fencing (Interfaccia SOAP)	fence_vmware_soap	Tabella A.24, «VMware Fencing (interfaccia SOAP) (Red Hat Enterprise Linux 6.2 e versioni più recenti)»
WTI Power Switch	fence_wti	Tabella A.25, «WTI Power Switch»

Tabella A.2, «APC Power Switch (telnet/SSH)» elenca i parametri del dispositivo di fencing usati da **`fence_apc`**, il fence agent per APC over telnet/SSH.

Tabella A.2. APC Power Switch (telnet/SSH)

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il dispositivo APC collegato al cluster nel quale il demone per il fencing esegue una registrazione tramite telnet/ssh.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Port IP (opzionale)	**`ipport`**	La porta TCP da usare per il collegamento al dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Power wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Porta	**`port`**	Porta TCP
Switch (opzionale)	**`switch`**	Il numero per l'interruttore APC che si collega al nodo se in presenza di interruttori multipli di tipo daisy-chained.
Use SSH	**`secure`**	Indica che il sistema utilizzerà SSH per accedere al dispositivo.

Campo di luci	Attributo `cluster.conf`	Descrizione
Percorso per SSH Identity File	**`identity_file`**	File di identità per SSH.

Tabella A.3, «APC Power Switch over SNMP» elenca i parametri del dispositivo di fencing usati da **`fence_apc_snmp`**, il fence agent per APC che esegue la registrazione nel dispositivo SNP tramite il protocollo SNMP.

Tabella A.3. APC Power Switch over SNMP

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il dispositivo APC collegato al cluster nel quale il demone per il fencing esegue una registrazione tramite il protocollo SNMP.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
UDP/TCP port	**`udpport`**	La porta UDP/TCP da usare per il collegamento con il dispositivo, il valore predefinito è 161.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
versione SNMP	**`snmp_version`**	La versione SNMP da usare (1, 2c, 3); il valore predefinito è 1.
Community SNMP	**`community`**	La stringa della comunità SNMP; il valore predefinito è **`private`**.
Livello di sicurezza SNMP	**`snmp_sec_level`**	Il livello di sicurezza SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocollo di autenticazione SNMP	**`snmp_auth_prot`**	Il protocollo di autenticazione SNMP (MD5, SHA).

Campo di luci	Attributo `cluster.conf`	Descrizione
Protocollo della privacy SNMP	**`snmp_priv_prot`**	Il protocollo di privacy SNMP (DES, AES).
Password del protocollo di privacy SNMP	**`snmp_priv_passwd`**	La password del protocollo di privacy SNMP.
Script del protocollo di privacy SNMP	**`snmp_priv_passwd_script`**	Lo script che fornisce la password per il protocollo di privacy SNMP. Il suo utilizzo sostituisce il parametro **Password del protocollo di privacy SNMP**.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Numero porta (Outlet)	**`port`**	Porta TCP

Tabella A.4, «Brocade Fabric Switch» elenca i parametri del dispositivo di fencing usati da **`fence_brocade`**, l'agente di fencing per gli interruttori Brocade FC.

Tabella A.4. Brocade Fabric Switch

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome per il dispositivo Brocade collegato al cluster.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP assegnato al dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Porta	**`port`**	Numero outlet dell'interruttore

Tabella A.5, «Cisco MDS» elenca i parametri del dispositivo di fencing usati da **`fence_cisco_mds`**, il fence agent per Cisco MDS.

Tabella A.5. Cisco MDS

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il dispositivo Cisco MDS 9000 con SNMP abilitato.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
UDP/TCP port	**`udpport`**	La porta UDP/TCP da usare per il collegamento con il dispositivo, il valore predefinito è 161.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Numero porta (Outlet)	**`port`**	Porta TCP
versione SNMP	**`snmp_version`**	La versione SNMP da usare (1, 2c, 3).
Community SNMP	**`community`**	La stringa della comunità SNMP.
Livello di sicurezza SNMP	**`snmp_sec_level`**	Il livello di sicurezza SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocollo di autenticazione SNMP	**`snmp_auth_prot`**	Il protocollo di autenticazione SNMP (MD5, SHA).
Protocollo della privacy SNMP	**`snmp_priv_prot`**	Il protocollo di privacy SNMP (DES, AES).
Password del protocollo di privacy SNMP	**`snmp_priv_passwd`**	La password del protocollo di privacy SNMP.
Script del protocollo di privacy SNMP	**`snmp_priv_passwd_script`**	Lo script che fornisce la password per il protocollo di privacy SNMP. Il suo utilizzo sostituisce il parametro **Password del protocollo di privacy SNMP**.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.

Campo di luci	Attributo `cluster.conf`	Descrizione

Tabella A.6, «Cisco UCS» elenca i parametri del dispositivo di fencing usati da **`fence_cisco_ucs`**, il fence agent per Cisco UCS.

Tabella A.6. Cisco UCS

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il dispositivo Cisco UCS.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
IP port (opzionale)	**`ipport`**	La porta TCP da usare per il collegamento al dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Usa SSH	**`ssl`**	Porta TCP da usare per il collegamento con il dispositivo.
Organizzazione -secondaria	**`suborg`**	Percorso aggiuntivo necessario per accedere alla organizzazione secondaria.
Numero porta (Outlet)	**`port`**	Nome della macchina virtuale
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.

Tabella A.7, «Dell DRAC 5» elenca i parametri del dispositivo di fencing usati da **`fence_drac5`**, il fence agent per Dell DRAC 5.

Tabella A.7. Dell DRAC 5

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome assegnato al DRAC.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al DRAC.
Port IP (opzionale)	**`ipport`**	La porta TCP da usare per il collegamento al dispositivo.
Login	**`login`**	Il nome di login usato per accedere al DRAC.
Password	**`passwd`**	La password usata per autenticare il collegamento al DRAC.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Use SSH	**`secure`**	Indica che il sistema userà SSH per accedere al dispositivo.
Percorso per SSH Identity File	**`identity_file`**	File di identità per SSH.
Nome modulo	**`module_name`**	(opzionale) Il nome del modulo per DRAC in presenza di moduli DRAC multipli.
Forza il prompt del comando	**`cmd_prompt`**	Il prompt del comando da usare. Il valore predefinito è '\$'.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.

Tabella A.8, «Eaton Network Power Controller (Interfaccia SNMP) (Red Hat Enterprise Linux 6.4 e versioni più recenti)» elenca i parametri del dispositivo di fencing usati da **`fence_eaton_snmp`**, il fence agent per l'interruttore di alimentazione della rete Eaton over SNMP.

Tabella A.8. Eaton Network Power Controller (Interfaccia SNMP) (Red Hat Enterprise Linux 6.4 e versioni più recenti)

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per l'interruttore di alimentazione di rete Eaton collegato al cluster.

Campo di luci	Attributo `cluster.conf`	Descrizione
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Porta UDP/TCP (opzionale)	**`udpport`**	La porta UDP/TCP da usare per il collegamento con il dispositivo, il valore predefinito è 161.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
versione SNMP	**`snmp_version`**	La versione SNMP da usare (1, 2c, 3); il valore predefinito è 1.
Community SNMP	**`community`**	La stringa della comunità SNMP; il valore predefinito è **`private`**.
Livello di sicurezza SNMP	**`snmp_sec_level`**	Il livello di sicurezza SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocollo di autenticazione SNMP	**`snmp_auth_prot`**	Il protocollo di autenticazione SNMP (MD5, SHA).
Protocollo della privacy SNMP	**`snmp_priv_prot`**	Il protocollo di privacy SNMP (DES, AES).
Password del protocollo di privacy SNMP	**`snmp_priv_passwd`**	La password del protocollo di privacy SNMP.
Script del protocollo di privacy SNMP	**`snmp_priv_passwd_script`**	Lo script che fornisce la password per il protocollo di privacy SNMP. Il suo utilizzo sostituisce il parametro **Password del protocollo di privacy SNMP**.
Power wait (secondi)	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Numero porta (Outlet)	**`port`**	Numero plug fisico o nome della macchina virtuale. Questo parametro è sempre necessario.

Tabella A.9, «Controllore Egenera SAN» elenca i parametri del dispositivo di fencing usati da **`fence_egenera`**, il fence agent per Egenera BladeFrame.

Tabella A.9. Controllore Egenera SAN

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il dispositivo Egenera BladeFrame collegato al cluster.
CServer	**`cserver`**	L'hostname (e facoltativamente il nome utente con il formato **`username@hostname`**) assegnato al dispositivo. Consultate la pagina man di fence_egenera(8) per maggiori informazioni.
Percorso ESH (opzionale)	**`esh`**	Il percorso per il comando esh su cserver (il default è /opt/panmgr/bin/esh)
Nome utente	**`user`**	Il nome di login. Il valore predefinito è **`root`**.
lpan	**`lpan`**	Il logical process area network (LPAN) del dispositivo.
pserver	**`pserver`**	Nome blade di processazione (pserver) del dispositivo.

Tabella A.10, «ePowerSwitch» elenca i parametri del dispositivo di fencing usati da **`fence_eps`**, il fence agent per ePowerSwitch.

Tabella A.10. ePowerSwitch

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il dispositivo ePowerSwitch collegato al cluster.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Nome della Pagina nascosta	**`hidden_page`**	Il nome della pagina nascosta per il dispositivo.

Campo di luci	Attributo `cluster.conf`	Descrizione
Numero porta (Outlet)	**`port`**	Numero di connessione fisica o nome della macchina virtuale.

Tabella A.11, «Fence virt» elenca i parametri del dispositivo di fencing usati da **`fence_virt`**, il fence agent per il dispositivo di fencing Fence virt.

Tabella A.11. Fence virt

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il dispositivo di fencing per Fence virt
Dispositivo Seriale	**`serial_device`**	Sull'host, il dispositivo seriale deve essere mappato in ogni file di configurazione del dominio. Per maggiori informazioni consultare la pagina man di **`fence_virt.conf`**. Se questo campo è stato specificato l'agente **`fence_virt`** opererà in modalità seriale. Se non si specifica alcun valore l'agente **`fence_virt`** opererà in modalità del canale VM.
Parametri Seriali	**`serial_params`**	I parametri seriali. Il valore predefinito è 115200, 8N1.
Indirizzo IP del canale VM	**`channel_address`**	Il canale IP. Il valore predefinito è 10.0.2.179.
Porta o Dominio (deprecato)	**`port`**	Macchina virtuale (nome o UUID del dominio) da isolare.
	`ipport`	La porta del canale. Il valore predefinito è 1229 che corrisponde al valore usato durante la configurazione del dispositivo di fencing con **luci**.

Tabella A.12, «Fujitsu Siemens Remoteview Service Board (RSB)» elenca i parametri del dispositivo di fencing usato da **`fence_rsb`**, il fence agent per Fujitsu-Siemens RSB.

Tabella A.12. Fujitsu Siemens Remoteview Service Board (RSB)

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per RSB da usare come dispositivo di fencing.

Campo di luci	Attributo `cluster.conf`	Descrizione
Hostname o indirizzo IP	**`ipaddr`**	L'hostname assegnato al dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Porta TCP	**`ipport`**	Il numero della porta sulla quale è in ascolto telnet. Il valore predefinito è 3172.

Tabella A.13, «HP BladeSystem (Red Hat Enterprise Linux 6.4 e versioni più recenti)» elenca i parametri del dispositivo di fencing usati da **`fence_hpblade`**, il fence agent per HP BladeSystem.

Tabella A.13. HP BladeSystem (Red Hat Enterprise Linux 6.4 e versioni più recenti)

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome assegnato al dispositivo HP BladeSystem collegato al cluster.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo HP BladeSystem.
Port IP (opzionale)	**`ipport`**	La porta TCP da usare per il collegamento al dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo HP BladeSystem. Questo parametro è necessario.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo di fencing.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Forza il prompt del comando	**`cmd_prompt`**	Il prompt del comando da usare. Il valore predefinito è '\$'.

Campo di luci	Attributo `cluster.conf`	Descrizione
Missing port ritorna OFF al posto di un errore	**`missing_as_off`**	Missing port ritorna OFF al posto di un errore.
Power Wait (secondi)	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Use SSH	**`secure`**	Indica che il sistema userà SSH per accedere al dispositivo.
Percorso per SSH Identity File	**`identity_file`**	File di identità per SSH.

Tabella A.14, «HP iLO/iLO2 (Integrated Lights Out)» elenca i parametri del dispositivo di fencing usati da **`fence_ilo`**, il fence agent per i dispositivi HP iLO.

Tabella A.14. HP iLO/iLO2 (Integrated Lights Out)

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il server con supporto HP iLO.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Port IP (opzionale)	**`ipport`**	Porta TCP da usare per il collegamento con il dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.

Tabella A.15, «HP iLO (Integrated Lights Out) MP» elenca i parametri del dispositivo di fencing usati da **`fence_ilo_mp`**, il fence agent per i dispositivi HP iLO MP.

Tabella A.15. HP iLO (Integrated Lights Out) MP

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il server con supporto HP iLO.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Port IP (opzionale)	**`ipport`**	Porta TCP da usare per il collegamento con il dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Use SSH	**`secure`**	Indica che il sistema userà SSH per accedere al dispositivo.
Percorso per SSH Identity File	**`identity_file`**	File di identità per SSH.
Forza il prompt del comando	**`cmd_prompt`**	Il prompt del comando da usare. Il valore predefinito è 'MP>', 'hpiLO->'.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.

Tabella A.16, «IBM BladeCenter» elenca i parametri del dispositivo di fencing usati da **`fence_bladecenter`**, il fence agent per IBM BladeCenter.

Tabella A.16. IBM BladeCenter

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome per il dispositivo IBM BladeCenter collegato al cluster.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
IP port (opzionale)	**`ipport`**	Porta TCP da usare per il collegamento con il dispositivo.

Campo di luci	Attributo `cluster.conf`	Descrizione
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Use SSH	**`secure`**	Indica che il sistema utilizzerà SSH per accedere al dispositivo.
Percorso per SSH Identity File	**`identity_file`**	File di identità per SSH.

Tabella A.17, «IBM BladeCenter SNMP» elenca i parametri del dispositivo di fencing usati da **`fence_ibmblade`**, il fence agent per IBM BladeCenter over SNMP.

Tabella A.17. IBM BladeCenter SNMP

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome per il dispositivo IBM BladeCenter SNMP collegato con il cluster.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Porta UDP/TCP (opzionale)	**`udpport`**	La porta UDP/TCP da usare per i collegamenti con il dispositivo, il valore predefinito è 161.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.

Campo di luci	Attributo cluster.conf	Descrizione
versione SNMP	**snmp_version**	La versione SNMP da usare (1, 2c, 3); il valore predefinito è 1.
Community SNMP	**community**	La stringa della comunità SNMP.
Livello di sicurezza SNMP	**snmp_sec_level**	Il livello di sicurezza SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocollo di autenticazione SNMP	**snmp_auth_prot**	Il protocollo di autenticazione SNMP (MD5, SHA).
Protocollo della privacy SNMP	**snmp_priv_prot**	Il protocollo di privacy SNMP (DES, AES).
SNMP privacy protocol password	**snmp_priv_passwd**	La password del protocollo di privacy SNMP.
Script del protocollo di privacy SNMP	**snmp_priv_passwd_script**	Lo script che fornisce la password per il protocollo di privacy SNMP. Il suo utilizzo sostituisce il parametro **Password del protocollo di privacy SNMP**.
Power Wait	**power_wait**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Porta	**port**	Numero di connessione fisica o nome della macchina virtuale.

Tabella A.18, «IBM iPDU (Red Hat Enterprise Linux 6.4 e versioni più recenti)» elenca i parametri del dispositivo di fencing usati da **fence_ipdu**, il fence agent per iPDU over SNMP.

Tabella A.18. IBM iPDU (Red Hat Enterprise Linux 6.4 e versioni più recenti)

Campo di luci	Attributo cluster.conf	Descrizione
Nome	**name**	Un nome per il dispositivo BM iPDU collegato al cluster nel quale il demone per il fencing esegue una registrazione tramite il protocollo SNMP.
Hostname o indirizzo IP	**ipaddr**	L'indirizzo IP o hostname assegnato al dispositivo.

Campo di luci	Attributo `cluster.conf`	Descrizione
UDP/TCP Port	**`udpport`**	La porta UDP/TCP da usare per il collegamento con il dispositivo, il valore predefinito è 161.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
versione SNMP	**`snmp_version`**	La versione SNMP da usare (1, 2c, 3); il valore predefinito è 1.
Community SNMP	**`community`**	La stringa della comunità SNMP; il valore predefinito è **`private`**.
Livello di sicurezza SNMP	**`snmp_sec_level`**	Il livello di sicurezza SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocollo di autenticazione SNMP	**`snmp_auth_prot`**	Il Protocollo di Autenticazione SNMP (MD5, SHA).
Protocollo della privacy SNMP	**`snmp_priv_prot`**	Il protocollo di privacy SNMP (DES, AES).
Password del protocollo di privacy SNMP	**`snmp_priv_passwd`**	La password del protocollo di privacy SNMP.
Script del protocollo di privacy SNMP	**`snmp_priv_passwd_script`**	Lo script che fornisce la password per il protocollo di privacy SNMP. Il suo utilizzo sostituisce il parametro **Password del protocollo di privacy SNMP**.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Porta	**`port`**	Porta TCP

Tabella A.19, «IF MIB» elenca i parametri del dispositivo di fencing usati da **`fence_ifmib`**, il fence agent per i dispositivi IF-MIB.

Tabella A.19. IF MIB

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome per il dispositivo IF MIB collegato al cluster.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Porta UDP/TCP (opzionale)	**`udpport`**	La porta UDP/TCP da usare per il collegamento con il dispositivo, il valore predefinito è 161.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
versione SNMP	**`snmp_version`**	La versione SNMP da usare (1, 2c, 3); il valore predefinito è 1.
Community SNMP	**`community`**	La stringa della comunità SNMP.
Livello di sicurezza SNMP	**`snmp_sec_level`**	Il livello di sicurezza SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocollo di autenticazione SNMP	**`snmp_auth_prot`**	Il protocollo di autenticazione SNMP (MD5, SHA).
Protocollo della privacy SNMP	**`snmp_priv_prot`**	Il protocollo di privacy SNMP (DES, AES).
Password del protocollo di privacy SNMP	**`snmp_priv_passwd`**	La password del protocollo di privacy SNMP.
Script del protocollo di privacy SNMP	**`snmp_priv_passwd_script`**	Lo script che fornisce la password per il protocollo di privacy SNMP. Il suo utilizzo sostituisce il parametro **Password del protocollo di privacy SNMP**.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Porta	**`port`**	Numero di connessione fisica o nome della macchina virtuale.

Campo di luci	Attributo `cluster.conf`	Descrizione

Tabella A.20, «Intel Modular» elenca i parametri del dispositivo di fencing usati da **`fence_intelmodular`**, il fence agent per Intel Modular.

Tabella A.20. Intel Modular

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome per il dispositivo Intel Modular collegato con il cluster.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
versione SNMP	**`snmp_version`**	La versione SNMP da usare (1, 2c, 3); il valore predefinito è 1.
Community SNMP	**`community`**	La stringa della comunità SNMP; il valore predefinito è **`private`**.
Livello di sicurezza SNMP	**`snmp_sec_level`**	Il livello di sicurezza SNMP (noAuthNoPriv, authNoPriv, authPriv).
Protocollo di autenticazione SNMP	**`snmp_auth_prot`**	Il protocollo di autenticazione SNMP (MD5, SHA).
Protocollo della privacy SNMP	**`snmp_priv_prot`**	Il protocollo di privacy SNMP (DES, AES).
Password del protocollo di privacy SNMP	**`snmp_priv_passwd`**	La password del protocollo di privacy SNMP.

Campo di luci	Attributo `cluster.conf`	Descrizione
Script del protocollo di privacy SNMP	**`snmp_priv_passwd_script`**	Lo script che fornisce la password per il protocollo di privacy SNMP. Il suo utilizzo sostituisce il parametro **Password del protocollo di privacy SNMP**.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Porta	**`port`**	Numero di connessione fisica o nome della macchina virtuale.

Tabella A.21, «IPMI (Intelligent Platform Management Interface) LAN» elenca i parametri del dispositivo di fencing usati da **`fence_ipmilan`**, il fence agent per IPMI over LAN.

Tabella A.21. IPMI (Intelligent Platform Management Interface) LAN

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome per il dispositivo IPMI LAN collegato con il cluster.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Login	**`login`**	Il nome di login di un utente in grado di emettere i comandi power on/off per la porta IPMI data.
Password	**`passwd`**	La password usata per autenticare il collegamento per la porta IPMI.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Tipo di autenticazione	**`auth`**	Tipo di autenticazione IPMI LAN: **`none`**, **`password`**, o **`md5`**.
Usa Lanplus	**`lanplus`**	**`True`** o **`1`**. Se vuoto, il valore è **`False`**.
Ciphersuite da usare	**`cipher`**	L'autenticazione del server remoto, l'integrità e gli algoritmi di cifratura da usare per i collegamenti lanplus IPMIv2.
Livello di privilegi	**`privlvl`**	Il livello di privilegi sul dispositivo IPMI.

Tabella A.22, «RHEV-M REST API (RHEL 6.2 e versione più recente, RHEV 3.0 e versione più recente)» elenca i parametri del dispositivo di fencing usati da **`fence_rhevm`**, il fence agent per RHEV-M REST API.

Tabella A.22. RHEV-M REST API (RHEL 6.2 e versione più recente, RHEV 3.0 e versione più recente)

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome del dispositivo di fencing RHEV-M REST API.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Port IP (opzionale)	**`ipport`**	Porta TCP da usare per il collegamento con il dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Usa SSH	**`ssl`**	Porta TCP da usare per il collegamento con il dispositivo.
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Porta	**`port`**	Numero di connessione fisica o nome della macchina virtuale.

Tabella A.23, «SCSI Fencing» elenca i parametri del dispositivo di fencing usati da **`fence_scsi`**, il fence agent per le prenotazioni persistenti SCSI.

NOTA

L'uso di SCSI persistent reservation come metodo di fencing è supportato con le seguenti limitazioni:

- Durante l'uso di SCSI fencing tutti i nodi nel cluster devono eseguire una registrazione con gli stessi dispositivi, così facendo ogni nodo è in grado di rimuovere la chiave di registrazione di un altro nodo da tutti i dispositivi sui quali è registrato.
- I dispositivi usati per i volumi del cluster devono essere un LUN completo e non partizioni. Le SCSI persistent reservation funzionano su di un intero LUN, ciò significa che l'accesso viene controllato per ogni LUN e non per singole partizioni.

Tabella A.23. SCSI Fencing

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Il nome per il dispositivo di SCSI fencing.
Nome del nodo		
Chiave per l'azione corrente		(annulla il nome del nodo)

Tabella A.24, «VMware Fencing (interfaccia SOAP) (Red Hat Enterprise Linux 6.2 e versioni più recenti)» elenca i parametri del dispositivo di fencing usati da **`fence_vmware_soap`**, il fence agent per VMWare over SOAP API.

Tabella A.24. VMware Fencing (interfaccia SOAP) (Red Hat Enterprise Linux 6.2 e versioni più recenti)

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`name`**	Un nome per il dispositivo di fencing della macchina virtuale.
Hostname o indirizzo IP	**`ipaddr`**	L'indirizzo IP o hostname assegnato al dispositivo.
Port IP (opzionale)	**`ipport`**	Porta TCP da usare per il collegamento con il dispositivo.
Login	**`login`**	Il nome per il login usato per accedere al dispositivo.
Password	**`passwd`**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**`passwd_script`**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Separatore	**`separator`**	Separatore per il CVS creato dall'elenco delle operazioni. Il valore predefinito è una virgola(,).
Power Wait	**`power_wait`**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Nome VM	**`port`**	Nome della macchina virtuale con formato del percorso dell'inventario (es. /datacenter/vm/Discovered_virtual_machine/myMachine).

Campo di luci	Attributo cluster.conf	Descrizione
VM UUID	**uuid**	L'UUID della macchina virtuale da isolare.
Usa SSH	**ssl**	Porta TCP da usare per il collegamento con il dispositivo.

Tabella A.25, «WTI Power Switch» elenca i parametri del dispositivo di fencing usati da **fence_wti**, il fence agent per l'interruttore di alimentazione della rete WTI.

Tabella A.25. WTI Power Switch

Campo di luci	Attributo cluster.conf	Descrizione
Nome	**name**	Un nome per il WTI power switch collegato al cluster.
Hostname o indirizzo IP	**ipaddr**	L'indirizzo dell'hostname o IP assegnato al dispositivo.
Port IP (opzionale)	**ipport**	La porta TCP da usare per il collegamento al dispositivo.
Login	**login**	Il nome per il login usato per accedere al dispositivo.
Password	**passwd**	La password usata per autenticare il collegamento al dispositivo.
Password Script (opzionale)	**passwd_script**	Lo script che fornisce una password per l'accesso al dispositivo per il fencing. Il suo utilizzo sostituisce il parametro **Password**.
Porta	**port**	Numero di connessione fisica o nome della macchina virtuale.
Prompt del comando Force	**cmd_prompt**	Il prompt del comando da usare. Il valore predefinito è ['RSM>', '>MPC', 'IPS>', 'TPS>', 'NBB>', 'NPS>', 'VMR>']
Power Wait	**power_wait**	Numero di secondi d'attesa dopo aver emesso un comando 'power off o power on'.
Use SSH	**secure**	Indica che il sistema utilizzerà SSH per accedere al dispositivo.
Percorso per SSH Identity File	**identity_file**	File di identità per SSH.

APPENDICE B. PARAMETRI DELLA RISORSA HA

La suddetta appendice fornisce le descrizioni dei parametri delle risorse HA. È possibile configurare i parametri con **luci** utilizzando il comando **ccs** o modificando **etc/cluster/cluster.conf**. Tabella B.1, «Sommario delle risorse HA» elenca le risorse, gli agenti corrispondenti ed i riferimenti ad altre tabelle per le descrizioni dei parametri. Per comprendere gli agenti delle risorse in modo dettagliato consultare **/usr/share/cluster** di qualsiasi nodo del cluster.

In aggiunta agli agenti descritti in questo appendice la directory **/usr/share/cluster** include uno script OCF di prova per un gruppo di risorse, **service.sh**. Per maggiori informazioni sui parametri inclusi in questo script consultare la script **service.sh**.

Per un elenco completo ed una descrizione degli attributi ed elementi **cluster.conf** consultare lo schema del cluster su **/usr/share/cluster/cluster.rng**, e **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (per esempio **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Tabella B.1. Sommario delle risorse HA

Risorse	Agente delle risorse	Riferimento alla descrizione del parametro
Apache	apache.sh	Tabella B.2, «Apache Server»
Istanza Condor	condor.sh	Tabella B.3, «Istanza Condor»
File System	fs.sh	Tabella B.4, «Filesystem»
File system GFS2	clusterfs.sh	Tabella B.5, «GFS2»
Indirizzo IP	ip.sh	Tabella B.6, «Indirizzo IP»
HA LVM	lvm.sh	Tabella B.7, «HA LVM»
MySQL	mysql.sh	Tabella B.8, «MySQL»
NFS Client	nfsclient.sh	Tabella B.9, «NFS Client»
NFS Export	nfsexport.sh	Tabella B.10, «NFS Export»
Server NFS	nfsserver.sh	Tabella B.11, «Server NFS»
NFS/CIFS Mount	netfs.sh	Tabella B.12, «NFS/CIFS Mount»
Open LDAP	openldap.sh	Tabella B.13, «Open LDAP»
Istanza di failover di Oracle 10g/11g	oracledb.sh	Tabella B.14, «Istanza di failover di Oracle 10g/11G»
Istanza di failover di Oracle 10g	orainstance.sh	Tabella B.15, «Istanza di failover di Oracle 10g»

Risorse	Agente delle risorse	Riferimento alla descrizione del parametro
Oracle 10g Listener	oralistener.sh	Tabella B.16, «Oracle 10g Listener»
PostgreSQL 8	postgres-8.sh	Tabella B.17, «PostgreSQL 8»
Database SAP	SAPDatabase	Tabella B.18, «Database SAP»
Istanza SAP	SAPInstance	Tabella B.19, «Istanza SAP»
Samba	samba.sh	Tabella B.20, «Server di Samba»
Script	script.sh	Tabella B.21, «Script»
Sybase ASE	ASEHAagent.sh	Tabella B.22, «Istanza di failover Sybase ASE»
Tomcat 6	tomcat-6.sh	Tabella B.23, «Tomcat 6»
Virtual Machine	vm.sh	Tabella B.24, «Virtual Machine» NOTA: **luci** lo riporterà come servizio virtuale se il cluster host supporta macchine virtuali.

Tabella B.2. Apache Server

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Il nome del servizio di Apache
Server Root	**`server_root`**	Il valore predefinito è **`/etc/httpd`**.
Config File	**`config_file`**	Specifica il file di configurazione di Apache. Il valore predefinito è **`/etc/httpd/conf`**.
Opzioni httpd	**`httpd_options`**	Altre opzioni della linea di comando per **`httpd`**.
Attesa arresto (secondi)	**`shutdown_wait`**	Specifica il numero di secondi da attendere per un arresto di tipo fine del servizio corretto.

Tabella B.3. Istanza Condor

Campo	Campo di luci	Attributo `cluster.conf`
Nome istanza	**`nome`**	Specifica un nome unico per l'istanza Condor.

Campo	Campo di luci	Attributo `cluster.conf`
Tipo di sottosistema Condor	**`tipo`**	Specifica il tipo di sottosistema Condor per questa istanza: **`schedd`**, **`job_server`**, o **`query_server`**.

Tabella B.4. Filesystem

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Specifica un nome per la risorsa del file system.
Tipo di filesystem	**`fstype`**	Se non specificato **`mount`** cercherà di determinare il tipo di file system.
Mount Point	**`mountpoint`**	Percorso nella gerarchia del file system per montare questo file system.
Dispositivo, etichetta FS, o UUID	**`dispositivo`**	Specifica il dispositivo associato con la risorsa del file system. Esso può essere un dispositivo a blocchi, una etichetta del file system o UUID di un file system.
Opzioni di montaggio	**`opzioni`**	Opzioni per il montaggio; cioè le opzioni usate per il montaggio del file system. Esse possono essere specifiche al file system. Consultare la pagina man di ***`mount`***_(8)_ per le opzioni supportate.
ID del File System (opzionale)	**`fsid`**	 **NOTA** Il ***`File System ID`*** è usato solo dai servizi NFS. Durante la creazione di una nuova risorsa del file system sarà possibile lasciare questo campo vuoto. Lasciando il campo vuoto l'ID del file system sarà assegnato automaticamente dopo aver confermato i parametri durante la configurazione. Se desiderate assegnare in modo esplicito un ID specificatelo in questo campo.
Force Unmount	**`force_unmount`**	Se abilitato forza lo smontaggio del file system. L'impostazione predefinita è ***`disabled`***. ***`Force Unmount`*** termina tutti i processi usando il mount point per liberare il mount durante il processo di smontaggio.
Forza fsck	**`force_fsck`**	Se abilitato causa l'esecuzione di **`fsck`** sul file system prima del montaggio. L'impostazione predefinita è ***`disabled`***.

Campo di luci	Attributo `cluster.conf`	Descrizione
Abilita il demone NFS ed il lockd workaround (Red Hat Enterprise Linux 6.4 e versioni più recenti)	**`nfsrestart`**	Se si esporta il file system tramite NFS e se talvolta si verificano problemi per un suo smontaggio (durante un arresto o un riposizionamento del servizio), impostando questa opzione non verranno considerati i riferimenti del file system prima di tale processo. Per utilizzare questa opzione abilitare **`Force unmount`** senza usare la suddetta opzione con la risorsa **`NFS Server`**. Impostare questa risorsa solo come ultima opzione disponibile, poichè essa risulta essere un processo critico per smontare il file system.
Utilizza il Quick Status Checks	**`quick_status`**	Se abilitato esegue i quick status checks.
Riavvia il nodo host se il processo di smontaggio fallisce	**`self_fence`**	Se abilitato riavvia il nodo se il processo di smontamento per questo file system fallisce. Il **`filesystem`** resource agent accetta il valore 1, **`yes`**, **`on`**, o **`true`** per abilitare questo parametro e un valore 0, **`no`**, **`off`**, o **`false`** per disabilitarlo. L'impostazione predefinita è ***`disabled`***.

Tabella B.5. GFS2

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Il nome della risorsa del file system.
Mount Point	**`mountpoint`**	Il percorse sul quale viene montata la risorsa del file system.
Dispositivo, etichetta FS, o UUID	**`dispositivo`**	Il file del dispositivo associato con la risorsa del file system.
Tipo di filesystem	**`fstype`**	Imposta su GFS2 su **luci**
Opzioni di montaggio	**`opzioni`**	Opzioni di montaggio.

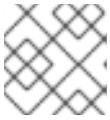
Campo di luci	Attributo cluster.conf	Descrizione
ID del File System (opzionale)	**fsid**	 **NOTA** Il ***File System ID*** è usato solo dai servizi NFS. Durante la creazione di una nuova risorsa del GFS2 sarà possibile lasciare questo campo vuoto. Lasciando il campo vuoto l'ID del file system sarà assegnato automaticamente dopo aver confermato i parametri durante la configurazione. Se desiderate assegnare in modo esplicito un ID specificatelo in questo campo.
Force Unmount	**force_unmount**	Se abilitato forza lo smontaggio del file system. L'impostazione predefinita è ***disabled***. ***Force Unmount*** termina tutti i processi usando il mount point per liberare il mount durante il processo di smontaggio. Con le risorse del GFS2 il mount point *non* viene smontato alla disattivazione del servizio a meno che ***Force Unmount*** è *abilitato*.
Abilita il demone NFS ed il lockd workaround (Red Hat Enterprise Linux 6.4 e versioni più recenti)	**nfsrestart**	Se si esporta il file system tramite NFS e se talvolta si verificano problemi per un suo smontaggio (durante un arresto o un riposizionamento del servizio), impostando questa opzione non verranno considerati i riferimenti del file system prima di tale processo. Per utilizzare questa opzione abilitare **Force unmount** senza usare la suddetta opzione con la risorsa **NFS Server**. Impostare questa risorsa solo come ultima opzione disponibile, poichè essa risulta essere un processo critico per smontare il file system.
Riavvia il nodo host se il processo di smontaggio fallisce	**self_fence**	Se abilitato ed il processo di smontamento per questo file system fallisce il nodo verrà immediatamente riavviato. Generalmente usato insieme al supporto force-unmount, ma non risulta essere necessario. Il **GFS2** resource agent accetta il valore 1, **yes**, **on**, o **true** per abilitare questo parametro e un valore 0, **no**, **off**, o **false** per disabilitarlo.

Tabella B.6. Indirizzo IP

Campo di luci	Attributo cluster.conf	Descrizione
Indirizzo IP, bit maschera di rete	**address**	L'indirizzo IP (e facoltativamente i bit della maschera di rete) per la risorsa. I bit della maschera di rete, o la lunghezza del prefisso della rete, si può posizionare dopo l'indirizzo stesso con una barra separatrice, soddisfando il formato CIDR (per esempio 10.1.1.1/8). Questo è un indirizzo IP virtuale. Gli indirizzi IPv4 e IPv6 sono supportati, insieme al monitoring del link NIC per ogni indirizzo IP.

Campo di luci	Attributo `cluster.conf`	Descrizione
Controlla link	**`monitor_link`**	Se abilitato causerà il fallimento del controllo dello stato se il link sul NIC al quale viene associato questo indirizzo IP non è presente.
Disabilita gli aggiornamenti per gli istradamenti statici	**`disable_rdisc`**	Disabilita gli aggiornamenti degli istradamenti usando il protocollo RDISC.
Numero di secondi di inattività (sleep) dopo la rimozione di un indirizzo IP	**`sleeptime`**	Specifica la quantità di tempo (in secondi) di inattività (sleep).

Tabella B.7. HA LVM

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Un nome unico per questa risorsa LVM.
Volume Group Name	**`vg_name`**	Un nome descrittivo del gruppo di volumi gestito.
Logical Volume Name (opzionale)	**`lv_name`**	Nome del volume logico gestito. Questo parametro è facoltativo se è presente più di un volume logico nel gruppo di volumi gestito.
Isola il nodo se non è in grado di rimuovere i tag LVM	**`self_fence`**	Isolare il nodo se non è in grado di rimuovere i tag LVM. L'agente delle risorse LVM accetta il valore 1 o **`yes`** per abilitare questo parametro, ed un valore 0 o **no** per disabilitarlo.

Tabella B.8. MySQL

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Specifica un nome della risorsa del server MySQL.

Campo di luci	Attributo `cluster.conf`	Descrizione
Config File	**`config_file`**	Specifica il file di configurazione. Il valore predefinito è **`/etc/my.cnf`**.
Listen Address	**`listen_address`**	Specifica un indirizzo IP per il server MySQL. Se non viene fornito un indirizzo IP verrà utilizzato il primo indirizzo IP del servizio.
Opzioni mysqld	**`mysqld_options`**	Altre opzioni della linea di comando per **`httpd`**.
Inizia attesa (secondi)	**`startup_wait`**	Specifica il numero di secondi da attendere per la fine corretta dell'avvio del servizio.
Attesa arresto (secondi)	**`shutdown_wait`**	Specifica il numero di secondi da attendere per un arresto di tipo fine del servizio corretto.

Tabella B.9. NFS Client

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Questo è un nome simbolico di un client usato per il riferimento nell'albero della risorsa. *Non* è equivalente all'opzione ***`Target`***.
Target Hostname, Wildcard, o Netgroup	**`target`**	Questo è il server dal quale si esegue il montaggio. Può essere specificato usando un hostnome, una wildcard (basata sull'hostname o indirizzo IP), o un netgroup che definisce gli host ai quali eseguire l'esportazione.
Permetti il ripristino di questo client NFS	**`allow_recover`**	Permette il ripristino.
Opzioni	**`opzioni`**	Definisce un elenco di opzioni per questo client — per esempio, i permessi aggiuntivi di accesso del client. Per maggiori informazioni consultate la pagina man di ***`exports`*** *(5)*, *Opzioni generali*.

Tabella B.10. NFS Export

Campo di luci	Attributo `cluster.conf`	Descrizione

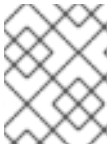
Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Nome descrittivo della risorsa. La risorsa di esportazione NFS assicura l'esecuzione corretta dei demoni NFS. È completamente riutilizzabile; generalmente è necessaria solo una risorsa di esportazione NFS.  **NOTA** Nominare la risorsa per l'esportazione NFS in modo da eseguire una distinzione netta da altre risorse NFS.

Tabella B.11. Server NFS

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Nome descrittivo della risorsa del server NFS. La suddetta risorsa è utile per il processo di esportazione dei file system NFSv4 sui client. A causa del modo in cui opera NFSv4, solo una risorsa NFSv4 può essere presente sul server in un dato momento. Altresì, non è possibile usare alcuna risorsa del server NFS se si utilizzano anche istanze locali di NFS su ogni nodo del cluster.

Tabella B.12. NFS/CIFS Mount

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Nome simbolico per il mount NFS o CIFS.  **NOTA** Questa risorsa è necessaria quando un servizio del cluster è configurato per essere un client NFS.
Mount Point	**`mountpoint`**	Il percorso sul quale la risorsa del file system è montato.
Host	**`host`**	Hostname o indirizzo IP del server NFS/CIFS.

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome della directory di esportazione NFS o condivisione CIFS	**`export`**	Nome della directory di esportazione NFS o nome della condivisione CIFS.
Tipo di filesystem	**`fstype`**	Tipo di file system: • ***`NFS`*** — Specifica l'uso della versione NFS predefinita. Questa è l'impostazione predefinita. • ***`NFS v4`*** — Specifica l'uso del protocollo NFSv4. • ***`CIFS`*** — Specifica l'uso del protocollo CIFS.
Force Unmount	**`force_unmount`**	Se ***`Force Unmount`*** è abilitato il cluster terminerà tutti i processi utilizzando questo file system all'arresto del servizio. Eseguendo tale processo il file system risulterà nuovamente disponibile. In caso contrario il processo di smontaggio fallirà ed il servizio sarà riavviato.
Non smontare il filesystem durante l'arresto di una operazione di riposizionamento.	**`no_unmount`**	Se abilitato indica che il file system non deve essere smontato durante una operazione di arresto o di riposizionamento.
Opzioni	**`opzioni`**	Opzioni di montaggio. Specifica un elenco di opzioni di montaggio. Se nessuna opzione viene specificata il file system viene montato con **`-o sync`**.

Tabella B.13. Open LDAP

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Specifica il nome di un servizio per il login ed altri processi.
Config File	**`config_file`**	Specifica un percorso assoluto per un file di configurazione. Il valore predefinito è **`/etc/openldap/slapd.conf`**.
Elenco URL	**`url_list`**	Il valore predefinito è **`ldap:///`**.

Campo di luci	Attributo `cluster.conf`	Descrizione
Opzioni **slapd**	**slapd_options**	Altre opzioni della linea di comando per **slapd**.
Attesa arresto (secondi)	**shutdown_wait**	Specifica il numero di secondi da attendere per un arresto di tipo fine del servizio corretto.

Tabella B.14. Istanza di failover di Oracle 10g/11G

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome istanza (SID) dell'istanza di Oracle	**nome**	Nome istanza.
Nome utente di Oracle	**user**	Questo è il nome utente dell'utente di Oracle usato dall'istanza AS di Oracle.
Home directory dell'applicazione di Oracle	**home**	Questa è la home directory di Oracle (applicazione, non utente). Configurata quando si installa Oracle.
Tipo di installazione di oracle	**tipo**	Tipo di installazione Oracle. Default: **10g**, Database Instance e Listener Only **base**, Database, Listener, Enterprise Manager, e ISQL*Plus: **base-em** (o **10g**), o Internet Application Server (infrastruttura): **ias** (o **10g-ias**).
Hostname virtuale (opzionale)	**vhost**	L'hostname virtuale che corrisponde all'hostname dell'installazione di Oracle 10g. Da notare che durante l'avvio/arresto di una risorsa oracledb, l'hostname verrà momentaneamente modificato e sarà implementato questo hostname. Per questo motivo configurare una risorsa oracledb solo come parte di un servizio esclusivo.

Tabella B.15. Istanza di failover di Oracle 10g

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome istanza (SID) dell'istanza di Oracle	**nome**	Nome istanza.

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome utente di Oracle	**`user`**	Questo è il nome utente dell'utente di Oracle usato dall'istanza di Oracle.
Home directory dell'applicazione di Oracle	**`home`**	Questa è la home directory di Oracle (applicazione, non utente). Configurata quando si installa Oracle.
Elenco di Oracle Listener (opzionale, separato da spazi)	**`listener`**	Elenco di Oracle listener che verranno avviati con l'istanza del database. I nomi sono separati da spazi. Esegue il default su nessun valore disabilitando così i listener.
Percorso per il Lock File (opzionale)	**`lockfile`**	Posizione del lockfile da usare per il controllo dell'esecuzione di Oracle. Esegue il default nella posizione sotto **`/tmp`**.

Tabella B.16. Oracle 10g Listener

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome listener	**`nome`**	Nome listener.
Nome utente di Oracle	**`user`**	Questo è il nome utente dell'utente di Oracle usato dall'istanza di Oracle.
Home directory dell'applicazione di Oracle	**`home`**	Questa è la home directory di Oracle (applicazione, non utente). Configurata quando si installa Oracle.

Tabella B.17. PostgreSQL 8

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Specifica il nome di un servizio per il login ed altri processi.
Config File	**`config_file`**	Definire un percorso assoluto per il file di configurazione. Il valore predefinito è **`/var/lib/pgsql/data/postgresql.conf`**.
Utente Postmaster	**`postmaster_user`**	Utente che esegue il server del database poichè non può essere eseguito dall'utente root. Il valore predefinito è postgres.

Campo di luci	Attributo `cluster.conf`	Descrizione
Opzioni Postmaster	**`postmaster_options`**	Altre opzioni della linea di comando per postmaster.
Attesa arresto (secondi)	**`shutdown_wait`**	Specifica il numero di secondi da attendere per un arresto di tipo fine del servizio corretto.

Tabella B.18. Database SAP

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome database SAP	**`SID`**	Specifica un identificatore del sistema SAP unico. Per esempio P01.
Directory eseguibile SAP	**`DIR_EXECUTABLE`**	Specifica il percorso completamente qualificato per **`sapstartsrv`** e **`sapcontrol`**.
Tipo di database	**`DBTYPE`**	Specifica uno dei seguenti tipi di database: Oracle, DB6, o ADA.
Nome di Oracle listener	**`NETSERVICENAME`**	Specifica il nome di Oracle TNS listener
Lo Stack ABAP non è installato, è installato solo lo Stack Java	**`DBJ2EE_ONLY`**	Se non avete installato uno stack ABAP nel database SAP, abilitare questo parametro.
Monitoraggio livello dell'applicazione	**`STRICT_MONITORING`**	Attiva il monitoraggio del livello dell'applicazione.
Ripristino avvio automatico	**`AUTOMATIC_RECOVER`**	Abilita o disabilita il ripristino avvio automatico.
Path per Java SDK	**`JAVE_HOME`**	Path per Java SDK.
Nome del file del driver JDBC	**`DB_JARS`**	Il nome del file del driver JDBC.

Campo di luci	Attributo `cluster.conf`	Descrizione
Percorso per uno scirpt di preavvio	**`PRE_START_USEREXIT`**	Percorso per uno script di preavvio.
Percorso per uno script Post-Start	**`POST_START_USEREXIT`**	Percorso per uno script post-start.
Percorso per uno script Pre-Stop	**`PRE_STOP_USEREXIT`**	Percorso per uno script pre-stop
Percorso per uno script Post-Stop	**`POST_STOP_USEREXIT`**	Percorso per uno script post-stop
Directory bootstrap dell'istanza J2EE	**`DIR_BOOTSTRAP`**	Il percorso completamente qualificato per la directory bootstrap dell'istanza J2EE. Per esempio **`/usr/sap/P01/J00/j2ee/cluster/bootstrap`**.
Percorso di archiviazione di sicurezza J2EE	**`DIR_SECSTORE`**	Il percorso completamente qualificato della directory di archiviazione di sicurezza J2EE. Per esempio **`/usr/sap/P01/SYS/global/security/lib/tools`**.

Tabella B.19. Istanza SAP

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome istanza SAP	**`InstanceName`**	Il nome dell'istanza SAP completamente qualificato. Per esempio P01_DVEBMGS00_sapp01ci.
Directory eseguibile SAP	**`DIR_EXECUTABLE`**	Il percorso completamente qualificato per **`sapstartsrv`** e **`sapcontrol`**.
La directory contenente il profilo SAP START	**`DIR_PROFILE`**	Il percorso completamente qualificato per il profilo SAP START.
Nome del profilo SAP START	**`START_PROFILE`**	Specifica il nome del profilo SAP START.

Campo di luci	Attributo `cluster.conf`	Descrizione
Numero di secondi in attesa prima di controllare lo stato dell'avvio	**START_WAIT TIME**	Specifica il numero di secondi da attendere prima di controllare lo stato dell'avvio (non aspetta J2EE-Addin).
Abilita il ripristino dell'avvio automatico	**AUTOMATIC_ RECOVER**	Abilita o disabilita il ripristino avvio automatico.
Percorso per uno scirpt di preavvio	**PRE_START_ USEREXIT**	Percorso per uno script di preavvio.
Percorso per uno script Post-Start	**POST_START _USEREXIT**	Percorso per uno script post-start.
Percorso per uno script Pre-Stop	**PRE_STOP_U SEREXIT**	Percorso per uno script pre-stop
Percorso per uno script Post-Stop	**POST_STOP_ USEREXIT**	Percorso per uno script post-stop

NOTA

In relazione alla Tabella B.20, «Server di Samba», durante la creazione o modifica di un servizio del cluster, collegare una risorsa del servizio-Samba direttamente al servizio, *non* alla risorsa all'interno del servizio.

Tabella B.20. Server di Samba

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**nome**	Specifica il nome del server di Samba.
Config File	**config_fil e**	File di configurazione di Samba

Campo di luci	Attributo `cluster.conf`	Descrizione
Altre opzioni della linea di comando per smbd	**`smbd_options`**	Altre opzioni della linea di comando per smbd.
Altre opzioni della line di comando per nmbd	**`nmbd_options`**	Altre opzioni della line di comando per nmbd.
Attesa arresto (secondi)	**`shutdown_wait`**	Specifica il numero di secondi da attendere per un arresto di tipo fine del servizio corretto.

Tabella B.21. Script

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome	**`nome`**	Specifica un nome per lo script dell'utente personalizzato. La risorsa dello script permette l'uso di uno init script LSB-conforme standard da usare per l'avvio del servizio clusterizzato.
Percorso completo per il file script	**`file`**	Inserire il percorso in corrispondenza di questo script personalizzato (per esempio **`/etc/init.d/`*`userscript`***).

Tabella B.22. Istanza di failover Sybase ASE

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome istanza	**`nome`**	Specifica il nome di una istanza della risorsa Sybase ASE.
Nome server ASE	**`server_name`**	Il nome del server ASE configurato per il servizio HA.
Home directory di SYBASE	**`sybase_home`**	La home directory dei prodotti Sybase.
File di login	**`login_file`**	Il percorso completo del file di login che contiene la coppia login-password.

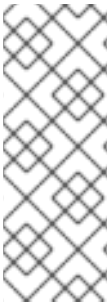
Campo di luci	Attributo cluster.conf	Descrizione
File delle interfacce	**interfaces_file**	Il percorso completo del file delle interfacce usato per avviare/accedere al server ASE.
Nome della directory SYBASE_ASE	**sybase_ase**	Il nome della directory sotto sybase_home dove sono installati tutti i prodotti ASE.
Nome directory SYBASE_OCS	**sybase_ocs**	Il nome della directory sotto sybase_home dove sono installati i prodotti OCS. Per esempio ASE-15_0.
Utente Sybase	**sybase_user**	L'utente in grado di eseguire il server ASE.
Start Timeout (secondi)	**start_timeout**	Il valore di start timeout.
Shutdown Timeout (secondi)	**shutdown_timeout**	Il valore di shutdown timeout.
Deep probe timeout	**deep_probe_timeout**	Il numero massimo di secondi in attesa per una risposta del server ASE prima di determinare se il server non ha inviato alcuna risposta durante l'esecuzione di deep probe.

Tabella B.23. Tomcat 6

Campo di luci	Attributo cluster.conf	Descrizione
Nome	**nome**	Specifica il nome di un servizio per il login ed altri processi.
Config File	**config_file**	Specifica il percorso assoluto per il file di configurazione. Il valore predefinito è **/etc/tomcat6/tomcat6.conf**.
Attesa arresto (secondi)	**shutdown_wait**	Specifica il numero di secondi d'attesa per l'arresto corretto fine del servizio. Il valore predefinito è 30.

IMPORTANTE

In relazione alla Tabella B.24, «Virtual Machine», durante la configurazione del cluster con le risorse della macchina virtuale utilizzare gli strumenti **`rgmanager`** per avviare ed arrestare le macchine virtuali. Se utilizzate **`virsh`** potreste causare l'esecuzione della macchina virtuale in più di una posizione, corrompendone i dati presenti al suo interno. Per informazioni sulla configurazione del sistema per ridurre la possibilità di un "avvio doppio" delle macchine virtuali da parte di un amministratore che utilizza strumenti cluster e non-cluster, consultare Sezione 2.14, «Configurazione di macchine virtuali in un ambiente clusterizzato».



NOTA

Le risorse della macchina virtuale sono configurate in modo diverso da altre risorse del cluster. Per configurare una risorsa della macchine virtuale utilizzando **luci**, aggiungere un gruppo di servizi al cluster e successivamente aggiungere una risorsa al servizio selezionando **`Macchina virtuale`** come tipo di risorsa, inserirendo i parametri della risorsa della macchina virtuale. Per informazioni su come configurare una macchina virtuale con **`ccs`**, consultare Sezione 5.12, «Risorse della macchina virtuale».

Tabella B.24. Virtual Machine

Campo di luci	Attributo `cluster.conf`	Descrizione
Nome del servizio	**`nome`**	Specifica il nome della macchina virtuale. Durante l'uso dell'interfaccia **luci** specificatelo come nome del servizio.
Avvia automaticamente questo servizio	**`autostart`**	Se abilitato la macchina virtuale viene avviata automaticamente dopo la formazione del quorum da parte del cluster. Se il parametro è *disabilitato* questa macchina virtuale *non* viene avviata automaticamente dopo che il cluster ha formato un quorum; la macchina virtuale viene messa in uno stato ***`disabled`***.
Esegui come esclusivo	**`exclusive`**	Se abilitata, questa macchina virtuale può essere riposizionata solo per l'esecuzione esclusiva su un altro nodo; cioè, per l'esecuzione su di un nodo senza altre macchine virtuali. Se nessun nodo è disponibile per l'esecuzione esclusiva di una macchina virtuale, il servizio non verrà riavviato dopo un eventuale fallimento. Altresì altre macchine virtuali non verranno automaticamente riposizionate sul nodo che esegue questa macchina virtuale come ***`Esegui come esclusivo`***. È possibile sovrascrivere questa opzione avviando manualmente o riposizionando le operazioni.
Dominio di failover	**`domain`**	Definisce un elenco di membri del cluster da provare nell'evento di un fallimento di una macchina virtuale.

Campo di luci	Attributo `cluster.conf`	Descrizione
Politica di ripristino	**`recovery`**	***`Recovery policy`*** fornisce le seguenti opzioni: • ***`Disable`*** — Disabilita la macchina virtuale se fallisce. • ***`Riposiziona`*** — Cerca di riavviare la macchina virtuale su un altro nodo; non prova ad eseguire il riavvio sul nodo corrente. • ***`Restart`*** — Cerca di riavviare localmente la macchina virtuale (nel nodo corrente) prima di riposizionare la macchina virtuale su un altro nodo. • ***`Restart-Disable`*** — Se fallisce il servizio verrà riavviato. Tuttavia se il riavvio del servizio fallisce il servizio stesso verrà disabilitato e non sarà spostato su un altro host presente nel cluster.
Opzioni di riavvio	**`max_restarts`**, **`restart_expire_time`**	Se selezionate **Riavvia** o **Riavvia-Disabilita** come politica di ripristino del servizio, sarà possibile specificare il numero massimo di fallimenti prima di eseguire il riposizionamento o disabilitare il servizio e specificare l'arco di tempo, espresso in secondi, dopo il quale dimenticare un processo di riavvio.
Tipo di migrazione	**`migrate`**	Specifica il tipo di migrazione ***`live`*** o ***`pause`***. L'impostazione predefinita è ***`live`***.
Mappatura di migrazione	**`migration_mapping`**	Specifica una interfaccia alternativa per la migrazione. Specificatelo quando per esempio l'indirizzo di rete usato per la migrazione della macchina virtuale su di un nodo, differisce dall'indirizzo del nodo usato per la comunicazione del cluster. Specificando il seguente durante la migrazione di una macchina virtuale da **`membro`** a **`membro2`**, la migrazione sarà eseguita effettivamente sul **`target2`**. In modo simile quando eseguito una migrazione da **`membro2`** a **`membro`**, la migrazione sarà fatta usando **`target`**. **`member:target,member2:target2`**
Status Program	**`status_program`**	Programma da eseguire in aggiunta al controllo standard per la presenza di una macchina virtuale. Se specificato il programma viene eseguito una sola volta al minuto. Così facendo sarete in grado di determinare lo stato dei servizi critici all'interno di una macchina virtuale. Per esempio, se una macchina virtuale esegue un web server il programma è in grado di controllare se il web server è in esecuzione; se il controllo fallisce (se ritorna un valore non-zero), la macchina virtuale viene recuperata. Dopo il riavvio di una macchina virtuale l'agente della risorsa eseguirà una chiamata periodica del programma dello stato attendendo un codice di ritorno corretto (zero) prima del ritorno. Tale operazione scadrà dopo cinque minuti.

Campo di luci	Attributo `cluster.conf`	Descrizione
Percorso per xmlfile usato per creare la VM	**`xmlfile`**	Percorso completo per il file XML **`libvirt`** contenente la definizione del dominio **`libvirt`**.
Percorso per il file di configurazione della VM	**`path`**	Una caratteristica del percorso delimitata da punteggiatura che il Virtual Machine Resource Agent (**`vm.sh`**) cerca per il file di configurazione della macchina virtuale. Per esempio: **`/mnt/guests/config:/etc/libvirt/qemu`**.  **IMPORTANTE** Il percorso non deve *mai* indicare direttamente ad un file di configurazione della macchina virtuale.
Percorso per la directory snapshot della VM	**`snapshot`**	Percorso per la directory snapshot dove verrà archiviata l'immagine della macchina virtuale.
URI dell'hypervisor	**`hypervisor_uri`**	URI dell'hypervisor (normalmente automatico).
URI per la migrazione	**`migration_uri`**	URI di migrazione (normalmente automatico)
Dati del tunnel attraverso ssh durante la migrazione	**`tunnelled`**	Dati tunnel attraverso ssh durante la migrazione.

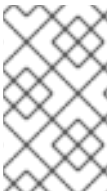
APPENDICE C. COMPORTAMENTO DELLE RISORSE HA

La suddetta appendice descrive il comportamento comune delle risorse ad elevata disponibilità (HA) e viene consultata per fornire informazioni ausiliare in grado di assistere l'utente alla configurazione dei servizi HA. Sarà possibile configurare i parametri con **luci** o attraverso la modifica di `etc/cluster/cluster.conf`. Per una descrizione dei parametri delle risorse HA consultare Appendice B, *Parametri della risorsa HA*. Per informazioni più dettagliate sugli agenti delle risorse consultare `/usr/share/cluster` di qualsiasi nodo del cluster.

NOTA

Per una comprensione dettagliata delle informazioni di questa appendice consultare anche gli agenti delle risorse ed il file di configurazione del cluster, `/etc/cluster/cluster.conf`.

Un servizio HA rappresenta un gruppo di risorse del cluster configurato in una entità omogenea in grado di fornire servizi specializzati ai client. Un servizio HA è rappresentato da un albero delle risorse nel file di configurazione del cluster, `/etc/cluster/cluster.conf` (in ogni nodo del cluster). Nel file di configurazione del cluster, ogni albero è una rappresentazione XML la quale specifica ogni risorsa, gli attributi e l'appartenenza tra le altre risorse presenti nell'albero delle risorse (genitore, figlio o altro tipo di parentela).



NOTA

Poichè un servizio HA consiste in risorse organizzate in un albero gerarchico, un servizio viene generalmente indicato come un *albero delle risorse* o *gruppo di risorse*. Entrambi sono sinonimi di *servizio HA*.

Alla radice di ogni albero delle risorse è presente un tipo speciale di risorsa — una *risorsa del servizio*. Altri tipi di risorse formano il resto del servizio determinando così le proprie caratteristiche. La configurazione di un servizio HA consiste nella creazione di una risorsa del servizio, creazione di risorse del cluster subordinate, ed organizzazione delle stesse in una entità omogenea conforme alle restrizioni gerarchiche del servizio.

Questa appendice consiste nelle seguenti sezioni:

- Sezione C.1, «Rapporti di parentela, genitore e figlio tra le risorse»
- Sezione C.2, «Ordine d'avvio dei parenti ed ordine della risorsa figlio»
- Sezione C.3, «Eredità, Il blocco delle <risorse>, ed il riutilizzo delle stesse»
- Sezione C.4, «Ripristino fallito ed alberi secondari indipendenti»
- Sezione C.5, «Servizi di debug e di prova ed ordine delle risorse»

NOTA

Le sezioni seguenti contengono gli esempi del file di configurazione del cluster, `/etc/cluster/cluster.conf`, solo a scopo di illustrazione.

C.1. RAPPORTI DI PARENTELA, GENITORE E FIGLIO TRA LE RISORSE

Il servizio di un cluster è una entità integrata eseguita sotto il controllo di **rgmanager**. Tutte le risorse in un servizio sono eseguite sullo stesso nodo. Dalla prospettiva di **rgmanager**, un servizio del cluster è una entità la quale può essere avviata, arrestata o riposizionata. Tuttavia all'interno di un servizio del cluster la gerarchia delle risorse determina l'ordine con il quale ogni risorsa viene avviata o arrestata. I livelli di gerarchia consistono in genitore, figlio, e parente.

Esempio C.1, «Gerarchia delle risorse del servizio foo» mostra un esempio di albero delle risorse del servizio *foo*. Nell'esempio i rapporti tra le risorse sono i seguenti:

- **fs:myfs** (<fs name="myfs" ...>) e **ip:10.1.1.2** (<ip address="10.1.1.2 .../>) sono imparentati.
- **fs:myfs** (<fs name="myfs" ...>) è il genitore di **script:script_child** (<script name="script_child"/>).
- **script:script_child** (<script name="script_child"/>) è il figlio di **fs:myfs** (<fs name="myfs" ...>).

Esempio C.1. Gerarchia delle risorse del servizio foo

```
<service name="foo" ...>
    <fs name="myfs" ...>
        <script name="script_child"/>
    </fs>
    <ip address="10.1.1.2" .../>
</service>
```

In un albero delle risorse le seguenti regole vengono applicate ai rapporti genitore/figlio:

- I genitori vengono avviati prima dei figli.
- Arrestare correttamente tutti i figli prima di poter arrestare un genitore.
- Per considerare una risorsa in buono stato tutte le risorse figlio devono avere uno stato corretto.

C.2. ORDINE D'AVVIO DEI PARENTI ED ORDINE DELLA RISORSA FIGLIO

La risorsa Service determina l'ordine d'avvio e di arresto di una risorsa figlio in base alla designazione di un attributo 'tipo-figlio' per una risorsa figlio nel modo seguente:

- Designa un attributo tipo-figlio (risorsa *tipo* figlio) — Se la risorsa Service designa un attributo tipo-figlio per una risorsa figlio, la risorsa in questione è classificata *tipo figlio*. L'attributo tipo-figlio determina in modo esplicito l'ordine d'avvio e di arresto della risorsa figlio.
- *Non designa* l'attributo tipo-figlio (risorsa di *tipo non* figlio) — Se la risorsa Service *non designa* un attributo tipo-figlio per una risorsa figlio, la risorsa in questione non è *tipo figlio*. La risorsa Service non controlla esplicitamente l'ordine d'avvio e d'arresto di una risorsa non di tipo figlio. Tuttavia una risorsa non di tipo figlio viene avviata ed arrestata in base al proprio ordine in **/etc/cluster.cluster.conf**. In aggiunta, le risorse non di tipo figlio vengono avviate dopo che tutte le risorse di tipo figlio sono state avviate ed arrestate prima dell'arresto delle risorse di tipo figlio.

NOTA

L'unica risorsa che implementa un ordine *tipo di risorsa figlio* è la risorsa Service.

Per maggiori informazioni sull'ordine d'avvio e arresto della risorsa di tipo figlio consultare Sezione C.2.1, «Ordine d'avvio e di arresto della risorsa di tipo figlio». Per maggiori informazioni sull'ordine d'avvio e arresto di una risorsa non di tipo figli consultare Sezione C.2.2, «Ordine di avvio ed arresto delle risorse non di tipo figlio».

C.2.1. Ordine d'avvio e di arresto della risorsa di tipo figlio

Per una risorsa di tipo figlio, l'attributo type definisce l'ordine d'avvio e di arresto per ogni tipo di risorsa con un numero da 1 a 100; un valore per l'avvio ed uno per l'arresto. Più basso è il numero e più alta è la priorità d'avvio o di arresto di una risorsa. Per esempio, Tabella C.1, «Ordine d'avvio e arresto del tipo di risorsa figlio» mostra i valori per l'avvio e l'arresto per ogni tipo di risorsa; Esempio C.2, «Valori d'avvio e di arresto della risorsa: Estratto dall'agente della risorsa Service, **`service.sh`**» mostra i valori per l'avvio e l'arresto come riportati dall'agente della risorsa Service, **`service.sh`**. Per la risorsa Service tutti i figli LVM sono avviati prima, seguiti da tutti i figli del file system, seguiti a loro volta da tutti i figli dello script e così via.

Tabella C.1. Ordine d'avvio e arresto del tipo di risorsa figlio

Risorse	Tipo figlio	Valore ordine d'avvio	Valore ordine d'arresto
LVM	lvm	1	9
File System	fs	2	8
File system GFS2	clusterfs	3	7
NFS Mount	netfs	4	6
NFS Export	nfsexport	5	5
NFS Client	nfsclient	6	4
Indirizzo IP	ip	7	2
Samba	smb	8	3
Script	script	9	1

Esempio C.2. Valori d'avvio e di arresto della risorsa: Estratto dall'agente della risorsa Service, `service.sh`

```
<special tag="rgmanager">
    <attributes root="1" maxinstances="1"/>
    <child type="lvm" start="1" stop="9"/>
    <child type="fs" start="2" stop="8"/>
    <child type="clusterfs" start="3" stop="7"/>
```

```
    <child type="netfs" start="4" stop="6"/>
    <child type="nfsexport" start="5" stop="5"/>
    <child type="nfsclient" start="6" stop="4"/>
    <child type="ip" start="7" stop="2"/>
    <child type="smb" start="8" stop="3"/>
    <child type="script" start="9" stop="1"/>
</special>
```

L'ordine all'interno di un tipo di risorsa viene conservato poichè presente all'interno del file di configurazione del cluster, **`/etc/cluster/cluster.conf`**. Per esempio considerate l'ordine d'avvio e di arresto delle risorse tipo figlio in Esempio C.3, «Ordine all'interno di un tipo di risorsa».

Esempio C.3. Ordine all'interno di un tipo di risorsa

```
<service name="foo">
  <script name="1" .../>
  <lvm name="1" .../>
  <ip address="10.1.1.1" .../>
  <fs name="1" .../>
  <lvm name="2" .../>
</service>
```

Ordine d'avvio della risorsa tipo figlio

In Esempio C.3, «Ordine all'interno di un tipo di risorsa» le risorse vengono avviate nel seguente ordine:

1. **`lvm:1`** — Questa è una risorsa LVM. Tutte le risorse LVM hanno una priorità più elevata e quindi avviate prima. **`lvm:1`** (**`<lvm name="1" .../>`**) è la prima risorsa avviata tra le risorse LVM poichè essa risulta essere la prima risorsa elencata nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

2. **`lvm:2`** — Questa è una risorsa LVM. Tutte le risorse LVM hanno una priorità più elevata e quindi avviate prima.. **`lvm:2`** (**`<lvm name="2" .../>`**) viene avviata dopo **`lvm:1`** poichè presente nell'elenco dopo **`lvm:1`** nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

3. **`fs:1`** — Questa è una risorsa del File System. Se presenti altre risorse del File System nella sezione *foo* del servizio esse verranno avviate in base all'ordine presente nell'elenco della sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

4. **`ip:10.1.1.1`** — Questa è una risorsa dell'Indirizzo IP. Se presenti altre risorse dell'indirizzo IP nella sezione *foo* del servizio, esse verranno avviate in base all'ordine presente nell'elenco della sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

5. **`script:1`** — Questa è una risorsa dello Script. Se sono presenti altre risorse dello Script nella sezione *foo* di Service, esse verranno avviate in base all'ordine presente nell'elenco della sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

Ordine d'arresto della risorsa tipo figlio

In Esempio C.3, «Ordine all'interno di un tipo di risorsa» le risorse vengono arrestate nel seguente ordine:

1. **`script:1`** — Questa è una risorsa dello Script. Se presenti altre risorse dello Script nella sezione *foo* di Service, esse verranno arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

2. **`ip:10.1.1.1`** — Questa è una risorsa dell'Indirizzo IP. Se presenti altre risorse dell'Indirizzo IP nella sezione *foo* del servizio, esse verranno arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

3. **`fs:1`** — Questa è una risorsa del File system. Se presenti altre risorse del File system nella sezione *foo* del servizio, esse verranno arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

4. **`lvm:2`** — Questa è una risorsa LVM. Tutte le risorse LVM vengono arrestate per ultime. **`lvm:2`** (**`<lvm name="2" .../>`**) viene arrestata prima di **`lvm:1`**; le risorse all'interno di un gruppo vengono arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

5. **`lvm:1`** — Questa è una risorsa LVM. Tutte le risorse LVM vengono arrestate per ultime. **`lvm:1`** (**`<lvm name="1" .../>`**) viene arrestata dopo **`lvm:2`**; le risorse all'interno di un gruppo vengono arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

C.2.2. Ordine di avvio ed arresto delle risorse non di tipo figlio

Sono presenti considerazioni aggiuntive per risorse di tipo non-figlio. Per una risorsa di tipo non-figlio l'ordine d'avvio e quello di arresto non sono specificati dalla risorsa Service. Al contrario i suddetti ordini vengono determinati in base all'ordine della risorsa figlio presente in **`/etc/cluster/cluster.conf`**. Altresì, le risorse di tipo non-figlio vengono avviate dopo le risorse di tipo figlio ed arrestate prima di qualsiasi risorsa figlio.

Per esempio, considerate l'ordine d'avvio e di arresto delle risorse non di tipo figlio in Esempio C.4, «Risorsa tipo figlio e non tipo figlio in un servizio».

Esempio C.4. Risorsa tipo figlio e non tipo figlio in un servizio

```
<service name="foo">
  <script name="1" .../>
  <nontypedresource name="foo"/>
  <lvm name="1" .../>
  <nontypedresourcetwo name="bar"/>
  <ip address="10.1.1.1" .../>
  <fs name="1" .../>
  <lvm name="2" .../>
</service>
```

Ordine d'avvio della risorsa non di tipo figlio

In Esempio C.4, «Risorsa tipo figlio e non tipo figlio in un servizio» le risorse figlio sono avviate nel seguente ordine:

1. **`lvm:1`** — Questa è una risorsa LVM. Tutte le risorse LVM hanno una priorità più elevata e quindi avviate prima. **`lvm:1`** (**`<lvm name="1" .../>`**) è la prima risorsa avviata tra le risorse LVM poichè essa risulta essere la prima risorsa elencata nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

2. **`lvm:2`** — Questa è una risorsa LVM. Tutte le risorse LVM hanno una priorità più elevata e quindi avviate prima.. **`lvm:2`** (**`<lvm name="2" .../>`**) viene avviata dopo **`lvm:1`** poichè presente nell'elenco dopo **`lvm:1`** nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

3. **`fs:1`** — Questa è una risorsa del File System. Se presenti altre risorse del File System nella sezione *foo* del servizio esse verranno avviate in base all'ordine presente nell'elenco della sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

4. **`ip:10.1.1.1`** — Questa è una risorsa dell'Indirizzo IP. Se presenti altre risorse dell'indirizzo IP nella sezione *foo* del servizio, esse verranno avviate in base all'ordine presente nell'elenco della sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

5. **`script:1`** — Questa è una risorsa dello Script. Se sono presenti altre risorse dello Script nella sezione *foo* di Service, esse verranno avviate in base all'ordine presente nell'elenco della sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

6. **`nontypedresource:foo`** — Questa è una risorsa non di tipo figlio. Per questo motivo essa verrà avviata dopo le risorse di tipo figlio. Altresì, la suddetta risorsa ha una priorità più alta rispetto all'altra risorsa, **`nontypedresourcetwo:bar`**; quindi verrà avviata prima di **`nontypedresourcetwo:bar`**. (Le risorse non di tipo figlio seguono un ordine d'avvio presente nella risorsa Service.)

7. **`nontypedresourcetwo:bar`** — Questa è una risorsa non di tipo figlio. Per questo motivo essa verrà avviata dopo le risorse di tipo figlio. Altresì, la suddetta risorsa ha una priorità più alta rispetto all'altra risorsa, **`nontypedresource:foo`**; quindi verrà avviata prima di **`nontypedresource:foo`**. (Le risorse non di tipo figlio seguono un ordine d'avvio presente nella risorsa Service.)

Ordine di arresto della risorsa non di tipo figlio

In Esempio C.4, «Risorsa tipo figlio e non tipo figlio in un servizio» le risorse figlio vengono arrestate nel seguente ordine:

1. **`nontypedresourcetwo:bar`** — Questa è una risorsa non di tipo figlio. Per questo motivo essa verrà arrestata prima delle risorse di tipo figlio. Altresì, la sua posizione nella risorsa Service viene dopo quella della risorsa di tipo non figlio, **`nontypedresource:foo`**; quindi verrà arrestata prima di **`nontypedresource:foo`**. (Le risorse non di tipo figlio vengono arrestate con un ordine inverso a quello presente nella risorsa Service.)

2. **`nontypedresource:foo`** — Questa è una risorsa non di tipo figlio e per questo motivo verrà arrestata prima delle risorse di tipo figlio. Altresì, la suddetta risorsa risulta avere una priorità più alta rispetto all'altra risorsa non di tipo figlio, **`nontypedresourcetwo:bar`**; quindi verrà arrestata dopo **`nontypedresourcetwo:bar`**. (Le risorse non di tipo figlio vengono arrestate nell'ordine inverso rispetto all'ordine presente nella risorsa Service.)

3. **`script:1`** — Questa è una risorsa dello Script. Se presenti altre risorse dello Script nella sezione *foo* di Service, esse verranno arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

4. **`ip:10.1.1.1`** — Questa è una risorsa dell'Indirizzo IP. Se presenti altre risorse dell'Indirizzo IP nella sezione *foo* del servizio, esse verranno arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

5. **`fs:1`** — Questa è una risorsa del File system. Se presenti altre risorse del File system nella sezione *foo* del servizio, esse verranno arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

6. **`lvm:2`** — Questa è una risorsa LVM. Tutte le risorse LVM vengono arrestate per ultime. **`lvm:2`** (**`<lvm name="2" .../>`**) viene arrestata prima di **`lvm:1`**; le risorse all'interno di un gruppo vengono arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

7. **`lvm:1`** — Questa è una risorsa LVM. Tutte le risorse LVM vengono arrestate per ultime. **`lvm:1`** (**`<lvm name="1" .../>`**) viene arrestata dopo **`lvm:2`**; le risorse all'interno di un gruppo vengono arrestate nell'ordine inverso all'ordine presente nella sezione *foo* del servizio di **`/etc/cluster/cluster.conf`**.

C.3. EREDITÀ, IL BLOCCO DELLE <RISORSE>, ED IL RIUTILIZZO DELLE STESSE

Alcune risorse possono ereditare i valori della risorsa genitore, ciò è comune nel caso di un servizio NFS. Esempio C.5, «Impostazione del servizio NFS per il riutilizzo e l'eredità della risorsa» mostra una configurazione del servizio NFS tipica ed una impostazione per l'utilizzo e l'eredità delle risorse.

Esempio C.5. Impostazione del servizio NFS per il riutilizzo e l'eredità della risorsa

```
¶
¶
    <resources>¶
        <nfsclient name="bob" target="bob.example.com"
options="rw,no_root_squash"/>¶
        <nfsclient name="jim" target="jim.example.com"
options="rw,no_root_squash"/>¶
        <nfsexport name="exports"/>¶
    </resources>¶
    <service name="foo">¶
        <fs name="1" mountpoint="/mnt/foo" device="/dev/sdb1"
fsid="12344">¶
            <nfsexport ref="exports">  <!-- nfsexport's path and fsid
attributes¶
                                       are inherited from the
mountpoint &¶
                                       fsid attribute of the
parent fs ¶
                                       resource -->¶
                <nfsclient ref="bob"/> <!-- nfsclient's path is
inherited from the¶
                                       mountpoint and the fsid
is added to the¶
                                       options string during
export -->¶
                <nfsclient ref="jim"/>¶
            </nfsexport>¶
```

```
        </fs>¶
        <fs name="2" mountpoint="/mnt/bar" device="/dev/sdb2"
fsid="12345">¶
            <nfsexport ref="exports">¶
                <nfsclient ref="bob"/> <!-- Because all of the critical
data for this¶
                                           resource is either
defined in the ¶
                                           resources block or
inherited, we can¶
                                           reference it again! -->¶
                <nfsclient ref="jim"/>¶
            </nfsexport>¶
        </fs>¶
        <ip address="10.2.13.20"/>¶
    </service>¶
¶
```

Se il servizio è solo (cioè senza alcun rapporto genitore/figlio), esso dovrà essere configurato nel modo seguente:

- Il servizio avrà bisogno di quattro risorse nfsclient — una per file system (un totale di due per file system), ed una per la macchina target (un totale di due per macchine target).
- Il servizio dovrà specificare il percorso di esportazione e l'ID del file system per ogni nfsclient, il quale introduce le modifiche per gli errori nella configurazione.

Tuttavia in Esempio C.5, «Impostazione del servizio NFS per il riutilizzo e l'eredità della risorsa» le risorse del client NFS *nfsclient:bob* e *nfsclient:jim* vengono definite una sola volta; similmente la risorsa di esportazione NFS *nfsexport:exports* viene definita una sola volta. Tutti gli attributi necessari dalle risorse sono ereditati dalla risorsa genitore. Poichè gli attributi ereditati sono dinamici (e non entrano in conflitto tra loro), sarà possibile utilizzare nuovamente le suddette risorse — ecco perchè esse vengono definite all'interno del blocco delle risorse. Potrebbe non essere pratico configurare alcune risorse in posizioni multiple, per esempio una risorsa del file system, poichè tale procedura potrebbe causare il montaggio di un file system su due nodi creando qualche problema.

C.4. RIPRISTINO FALLITO ED ALBERI SECONDARI INDIPENDENTI

In molti ambienti enterprise il corso normale delle azioni per un ripristino fallito di un servizio è quello di avviare l'intero servizio se qualsiasi componente dello stesso fallisce. Per esempio in Esempio C.6, «Ripristino normale del servizio *foo* fallito» se uno degli script definiti in questo servizio fallisce, il corso normale delle azioni è quello di riavviare (riposizionere o disabilitare, in base alla politica di ripristino del servizio) il servizio. Potrà essere necessario riavviare solo parte del servizio prima di tentare un'azione di ripristino. Per fare questo usare l'attributo ***__independent_subtree***. Per esempio in Esempio C.7, «Ripristino errore servizio *foo* con l'attributo ***__independent_subtree***» l'attributo ***__independent_subtree*** viene usato per eseguire le suddette azioni:

- Se script:script_one fallisce, riavviare script:script_one, script:script_two, e script:script_three.
- Se script:script_two fallisce, riavviare solo script:script_two.
- Se script:script_three fallisce, riavviare script:script_one, script:script_two, e script:script_three.
- Se script:script_four fallisce, riavviare l'intero servizio.

Esempio C.6. Ripristino normale del servizio *foo* fallito

```
<service name="foo">
      <script name="script_one" ...>
          <script name="script_two" .../>
      </script>
      <script name="script_three" .../>
</service>
```

Esempio C.7. Ripristino errore servizio *foo* con l'attributo *__independent_subtree*

```
<service name="foo">
      <script name="script_one" __independent_subtree="1" ...>
          <script name="script_two" __independent_subtree="1" .../>
          <script name="script_three" .../>
      </script>
      <script name="script_four" .../>
</service>
```

In alcune circostanze se un componente di un servizio fallisce sarà possibile disabilitarlo senza disabilitare l'intero servizio, e quindi senza interessare altri servizi che utilizzano i componenti del servizio stesso. Con Red Hat Enterprise Linux 6.1 sarà possibile eseguire questa operazione utilizzando ***__independent_subtree="2"*** il quale designa l'albero indipendente come non-critico.

NOTA

Usare solo un flag non-critico su risorse con un solo riferimento. Il flag non-critico funziona con tutte le risorse su tutti i livelli dell'albero ma non deve essere usato sul livello superiore durante la definizione dei servizi o delle macchine virtuali.

Con Red Hat Enterprise Linux 6.1 sarà possibile impostare all'interno dell'albero delle risorse le scadenze per il riavvio ed il riavvio massimo per il nodo per alberi secondari indipendenti. Per impostare i suddetti limiti usare i seguenti attributi:

- **`__max_restarts`** configura il numero massimo di riavvii tollerati prima di arrestarsi.
- **`__restart_expire_time`** configura la quantità di tempo, in secondi, dopo il quale non verrà più eseguito un tentativo di riavvio.

C.5. SERVIZI DI DEBUG E DI PROVA ED ORDINE DELLE RISORSE

È possibile eseguire il debug ed il test dei servizi ed ordinare le risorse con l'utilità **`rg_test`**. **`rg_test`** è una utilità della linea di comando resa disponibile dal pacchetto **`rgmanager`** eseguita dalla shell o dal terminale (non è disponibile in **Conga**). Tabella C.2, «Riassunto utilità **`rg_test`**» riassume le azioni e la sintassi per l'utilità **`rg_test`**.

Tabella C.2. Riassunto utilità `rg_test`

Azione	Sintassi
Mostra le regole della risorsa in grado di comprendere **rg_test**.	**rg_test rules**
Esegue una prova della configurazione (e /usr/share/cluster) ed esegue una ricerca degli errori o degli agenti della risorsa ridondante.	**rg_test test /etc/cluster/cluster.conf**
Mostra l'ordine d'avvio e di arresto di un servizio	Mostra l'ordine d'avvio: **rg_test noop /etc/cluster/cluster.conf start service *servicename*** Mostra l'ordine di arresto: **rg_test noop /etc/cluster/cluster.conf stop service *servicename***
Avvia o arresta esplicitamente un servizio.	 **IMPORTANTE** Esegue questa azione solo su di un nodo e disabilita sempre prima il servizio in rgmanager. Avviare un servizio: **rg_test test /etc/cluster/cluster.conf start service *servicename*** Arrestare un servizio: **rg_test test /etc/cluster/cluster.conf stop service *servicename***

Azione	Sintassi
Calcola e visualizza il delta dell'albero delle risorse tra due file cluster.conf.	**rg_test delta *cluster.conf file 1* *cluster.conf file 2*** Per esempio: **rg_test delta /etc/cluster/cluster.conf.bak /etc/cluster/cluster.conf**

APPENDICE D. CONTROLLO RISORSE SERVIZIO DEL CLUSTER E TIMEOUT DEL FAILOVER

Questa appendice descrive il processo di monitoraggio dello stato delle risorse del cluster da perte di **rgmanager**, e la modifica dell'intervallo di controllo dello stato. Inoltre l'appendice descrive anche il parametro del servizio **__enforce_timeouts** il quale indica che un timeout di una operazione potrebbe causare il fallimento del servizio.

NOTA

Per comprendere in modo adeguato questa appendice è necessario conoscere in maniera dettagliata gli agenti delle risorse ed il file di configurazione del cluster, **/etc/cluster/cluster.conf**. Per un elenco completo ed una descrizione degli attributi e degli elementi **cluster.conf** consultate lo schema disponibile su **/usr/share/cluster/cluster.rng** e lo schema **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (per esempio **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

D.1. MODIFICA DELL'INTERVALLO DI CONTROLLO DELLO STATO DELLE RISORSE

rgmanager controlla lo stato delle singole risorse e non dell'intero servizio. Ogni 10 secondi rgmanager esegue la scansione dell'albero delle risorse andando alla ricerca di quelle risorse che hanno passato il proprio intervallo di "controllo dello stato".

Ogni agente delle risorse specifica la quantità di tempo che intercorre tra i controlli periodici dello stato. Ogni risorsa utilizza i valori di timeout se non diversamente indicato nel file **cluster.conf** usando il tag speciale **<action>**:

```
<action name="status" depth="*" interval="10" />
```

Questo tag risulta essere un figlio speciale della risorsa nel file **cluster.conf**. Per esempio, se siete in possesso di una risorsa del file system per la quale desiderate sovrascrivere l'intervallo di controllo dello stato, allora specificare la risorsa del file system nel file **cluster.conf** nel modo seguente:

```
<fs name="test" device="/dev/sdb3">
  <action name="status" depth="*" interval="10" />
  <nfsexport...>
  </nfsexport>
</fs>
```

Alcuni agenti forniscono valori "depths" multipli di controllo. Per esempio, in un controllo normale dello stato del file system (depth 0) sarà possibile controllare se il file system è stato montato nella posizione corretta. Un controllo più dettagliato presenta un valore depth 10, con il quale si verifica la possibile lettura di un file dal file system. Con un valore depth 20 si verifica la possibilità di scrittura di un file system. Nell'esempio di seguito riportato **depth** è stato impostato su *****, il quale indica che questi valori devono essere usati per tutti i parametri depth. Ne risulta che il file system **test** viene controllato con il valore più alto di depth fornito dall'agente delle risorse (in questo caso 20) ogni 10 secondi.

D.2. COME IMPORRE I TIMEOUT DELLE RISORSE

Per i processi di avvio, arresto e failover delle risorse non è presente alcun timeout. Alcune risorse hanno bisogno di un timeout molto lungo per il loro avvio o arresto. Sfortunatamente un fallimento del processo di arresto di una risorsa (incluso un timeout) rende il servizio non operativo (fallito). È possibile, se desiderate, forzare un timeout su ogni risorsa in un servizio aggiungendo **__enforce_timeouts="1"** nel file **cluster.conf**.

Il seguente esempio mostra un servizio del cluster configurato con l'attributo **__enforce_timeouts** impostato per la risorsa **netfs**. Se è stato impostato il suddetto attributo ed il processo di arresto richiede un periodo di tempo maggiore a 30 secondi per smontare il file system NFS durante un processo di ripristino, l'operazione scadrà attribuendo al servizio lo stato di fallito.

```
</screen>
<rm>
  <failoverdomains/>
  <resources>
    <netfs export="/nfstest" force_unmount="1" fstype="nfs"
host="10.65.48.65"
          mountpoint="/data/nfstest" name="nfstest_data"
options="rw,sync,soft"/>
  </resources>
  <service autostart="1" exclusive="0" name="nfs_client_test"
recovery="relocate">
    <netfs ref="nfstest_data" __enforce_timeouts="1"/>
  </service>
</rm>
```

APPENDICE E. SOMMARIO DEI TOOL DELLA LINEA DI COMANDO

Tabella E.1, «Sommario del tool della linea di comando» riassume i tool della linea di comando preferiti per la configurazione e gestione di High Availability Add-On. Per maggiori informazioni sui comandi e le variabili consultate la pagina man per ogni tool della linea di comando.

Tabella E.1. Sommario del tool della linea di comando

Tool della linea di comando	Usato con	Scopo
`ccs_config_dump` — Tool per il dump della configurazione del cluster	Infrastruttura del cluster	**`ccs_config_dump`** genera gli output XML della configurazione in esecuzione. La configurazione in esecuzione è, talvolta, diversa da quella archiviata sul file poichè alcuni sottosistemi archiviano o impostano le informazioni predefinite all'interno della configurazione. Questi valori sono generalmente presenti sulla versione sul-disco della configurazione ma sono necessari al momento dell'esecuzione per un funzionamento corretto del cluster. Per maggiori informazioni su questo tool consultare la pagina man ccs_config_dump(8).
`ccs_config_validate` — Tool per la convalida della configurazione del cluster	Infrastruttura del cluster	**`ccs_config_validate`** convalida **`cluster.conf`** nei confronti dello schema, **`cluster.rng`** (posizionato in **`/usr/share/cluster/cluster.rng`** su ogni nodo). Per maggiori informazioni su questo tool consultare la pagina man di ccs_config_validate(8).
`clustat` — Utilità sullo stato del cluster	Componenti per la gestione del servizio ad elevata disponibilità	Il comando **`clustat`** visualizza lo stato del cluster. Esso mostra le informazioni di appartenenza, il quorum e lo stato di tutti i servizi configurati. Per maggiori informazioni su questo tool consultare la pagina man di clustat(8).
`clusvcadm` — Utilità per l'amministrazione dei servizi dell'utente del cluster	Componenti per la gestione del servizio ad elevata disponibilità	Il comando **`clusvcadm`** permette all'utente di abilitare, disabilitare, riposizionare e riavviare i servizi ad elevata disponibilità in un cluster. Per maggiori informazioni su questo tool consultare la pagina man di clusvcadm(8).

Tool della linea di comando	Usato con	Scopo
cman_tool — Tool di gestione del cluster	Infrastruttura del cluster	**cman_tool** è un programma in grado di gestire il CMAN cluster manager. Esso fornisce la capacità di unirsi ad un cluster, di abbandonare un cluster, di terminare un nodo o modificare i voti del quorum attesi di un nodo in un cluster. Per maggiori informazioni su questo tool consultare la pagina man di cman_tool(8).
fence_tool — Tool per il fencing	Infrastruttura del cluster	**fence_tool** è un programma usato per entrare ed uscire dal dominio di fencing. Per maggiori informazioni su questo tool consultare la pagina man di fence_tool(8).

APPENDICE F. HIGH AVAILABILITY LVM (HA-LVM)

Red Hat High Availability Add-On fornisce il supporto per i volumi LVM ad elevata disponibilità (HA-LVM) in una configurazione di failover. Ciò risulta essere diverso da una configurazione attiva/attiva abilitata dal Clustered Logical Volume Manager (CLVM), il quale rappresenta un insieme di estensioni clusterizzate per LVM che permettono ad un cluster di computer di gestire lo storage condiviso.

In base alle necessità dei servizi o delle applicazioni implementate utilizzare CLVM o HA-LVM.

- Se le applicazioni sono compatibili con i cluster ed in grado di essere eseguite simultaneamente su macchine multipli, allora è consigliato utilizzare CLVM. In particolare, se più nodi presenti nel cluster necessitano di un accesso allo storage condiviso tra i nodi attivi, allora sarà imperativo utilizzare CLVM. CLVM permette ad un utente di configurare i volumi logici sullo storage condiviso bloccando l'accesso allo storage fisico durante la configurazione di un volume logico, ed utilizza i servizi di blocco clusterizzati per gestire lo storage condiviso. Per informazioni su CLVM e sulla configurazione di LVM, consultare il *Logical Volume Manager Administration*.

- Se le applicazioni vengono eseguite in maniera ottimale in configurazioni attiva/passiva (failover), dove il solo nodo in grado di accedere allo storage risulta essere attivo in un determinato momento, in questo caso utilizzare High Availability Logical Volume Management (HA-LVM).

La maggior parte delle applicazioni vengono eseguite al meglio con una configurazione attiva/passiva poichè esse non sono state create o ottimizzate per l'esecuzione con altre istanze. La scelta di eseguire una applicazione non compatibile con il cluster su volumi logici clusterizzati, potrebbe impattare negativamente sulle prestazioni se il volume logico è speculare. Tale situazione si verifica in presenza di un sovraccarico delle informazioni nelle comunicazioni del cluster per i volumi logici in queste istanze. Un'applicazione compatibile con il cluster dovrà essere in grado di migliorare le proprie prestazioni rispetto alle perdite di prestazioni introdotte dai file system e dai volumi logici conformi al cluster. Questo è più facilmente raggiungibile per alcune applicazioni e carichi di lavoro. Per poter scegliere tra le due varianti di LVM, determinare i requisiti del cluster e gli sforzi aggiuntivi per l'ottimizzazione ad un cluster attivo/attivo. Molti utenti ottengono i migliori risultati utilizzando HA-LVM.

HA-LVM e CLVM sono simili in quanto essi impediscono la corruzione dei metadati LVM e dei volumi logici. Tale situazione si può verificare se macchine multiple sono in grado di eseguire le modifiche. HA-LVM impone una restrizione in grado di permettere ad un solo volume logico di essere attivato in modo esclusivo; e cioè, attivo su una sola macchina per volta. Così facendo verranno usate solo implementazioni locali (non-clusterizzate) dei driver dello storage. Evitando l'overhead del cluster si potrà migliorare le prestazioni. CLVM non impone queste restrizioni - un utente è libero di attivare un volume logico su tutte le macchine presenti in un cluster; così facendo verrà forzato l'utilizzo di driver dello storage compatibili con il cluster, e quindi di applicazioni e file system compatibili con il cluster.

HA-LVM può essere impostato in modo da usare uno dei due metodi per l'attivazione esclusiva del volume logico.

- Il metodo preferito utilizza CLVM, in questo modo i volumi logici saranno attivati solo in modo esclusivo. Uno dei vantaggi è rappresentato da una impostazione più semplice e migliore prevenzione di errori amministrativi (come ad esempio la rimozione di un volume logico in uso). Per poter usare CLVM, il software Resilient Storage Add-On e High Availability Add-On, incluso il demone **`clvmd`**, devono essere in esecuzione.

  La procedura per la configurazione di HA-LVM usando questo metodo è descritta in Sezione F.1, «Configurazione di HA-LVM Failover con CLVM (preferito)» .

- Il secondo metodo utilizza i "tag" LVM ed il blocco della macchina locale. Questo metodo presenta il vantaggio di non richiedere alcun pacchetto LVM; tuttavia sono presenti un numero

maggiore di fasi per la sua impostazione e non impedisce all'amministratore la possibilità di rimuovere accidentalmente un volume logico da un nodo presente nel cluster quando non risulta attivo. La procedura per la configurazione di HA-LVM usando questo metodo viene descritta in Sezione F.2, «Configurazione HA-LVM Failover con l'uso di tag».

F.1. CONFIGURAZIONE DI HA-LVM FAILOVER CON CLVM (PREFERITO)

Per impostare un HA-LVM failover (utilizzando la variante CLVM preferita), eseguire le seguenti fasi:

1. Assicuratevi che il sistema sia configurato per supportare CLVM:
   - L'High Availability Add-On ed il Resilient Storage Add-On devono essere installati, incluso il pacchetto **`cmirror`** se i volumi logici CLVM devono essere speculari.
   - Il parametro **`locking_type`** nella sezione globale del file **`/etc/lvm/lvm.conf`** deve avere un valore '3'.
   - L'High Availability Add-On ed il Resilient Storage Add-On software, incluso il demone **`clvmd`**, devono essere in esecuzione. Per il mirroring CLVM, anche il servizio **`cmirrord`** deve essere in esecuzione.
2. Creare il volume logico ed il file system usando LVM standard ed i comandi del file system come riportato nel seguente esempio.

```
# pvcreate /dev/sd[cde]1

# vgcreate -cy shared_vg /dev/sd[cde]1

# lvcreate -L 10G -n ha_lv shared_vg

# mkfs.ext4 /dev/shared_vg/ha_lv

# lvchange -an shared_vg/ha_lv
```

   Per informazioni sulla creazione dei volumi logici LVM consultate la *Logical Volume Manager Administration*.

3. Modificare il file **`/etc/cluster/cluster.conf`** in modo da includere il volume logico appena creato come risorsa in uno dei seguenti servizi. Alternativamente usare **Conga** o il comando **`ccs`** per configurare le risorse del file system e LVM per il cluster. Di seguito viene riportato un esempio di sezione del gestore delle risorse del file **`/etc/cluster/cluster.conf`** che configura un volume logico CLVM come risorsa del cluster:

```
<rm>
   <failoverdomains>
       <failoverdomain name="FD" ordered="1" restricted="0">
          <failoverdomainnode name="neo-01" priority="1"/>
          <failoverdomainnode name="neo-02" priority="2"/>
       </failoverdomain>
   </failoverdomains>
   <resources>
       <lvm name="lvm" vg_name="shared_vg" lv_name="ha-lv"/>
       <fs name="FS" device="/dev/shared_vg/ha-lv" force_fsck="0"
```

```
force_unmount="1" fsid="64050" fstype="ext4" mountpoint="/mnt"
options="" self_fence="0"/>
   </resources>
   <service autostart="1" domain="FD" name="serv"
recovery="relocate">
       <lvm ref="lvm"/>
       <fs ref="FS"/>
   </service>
</rm>
```

F.2. CONFIGURAZIONE HA-LVM FAILOVER CON L'USO DI TAG

Per impostare HA-LVM failover usando i tag nel file **/etc/lvm/lvm.conf** seguire le fasi di seguito riportate:

1. Assicuratevi che il parametro **locking_type** nella sezione globale del file **/etc/lvm/lvm.conf** sia stato impostato con un valore '1'.

2. Creare il volume logico ed il file system usando LVM standard ed i comandi del file system come riportato nel seguente esempio.

   ```
   # pvcreate /dev/sd[cde]1

   # vgcreate shared_vg /dev/sd[cde]1

   # lvcreate -L 10G -n ha_lv shared_vg

   # mkfs.ext4 /dev/shared_vg/ha_lv
   ```

   Per informazioni sulla creazione dei volumi logici LVM consultate la *Logical Volume Manager Administration*.

3. Modificare il file **/etc/cluster/cluster.conf** in modo da includere il volume logico appena creato come risorsa in uno dei seguenti servizi. Alternativamente usare **Conga** o il comando **ccs** per configurare le risorse del file system e LVM per il cluster. Di seguito viene riportato un esempio di sezione del gestore delle risorse del file **/etc/cluster/cluster.conf** che configura un volume logico CLVM come risorsa del cluster:

   ```
   <rm>
      <failoverdomains>
          <failoverdomain name="FD" ordered="1" restricted="0">
             <failoverdomainnode name="neo-01" priority="1"/>
             <failoverdomainnode name="neo-02" priority="2"/>
          </failoverdomain>
      </failoverdomains>
      <resources>
          <lvm name="lvm" vg_name="shared_vg" lv_name="ha_lv"/>
          <fs name="FS" device="/dev/shared_vg/ha_lv" force_fsck="0"
   force_unmount="1" fsid="64050" fstype="ext4" mountpoint="/mnt"
   options="" self_fence="0"/>
      </resources>
      <service autostart="1" domain="FD" name="serv"
   recovery="relocate">
   ```

```
        <lvm ref="lvm"/>
        <fs ref="FS"/>
    </service>
</rm>
```

NOTA

In presenza di volumi logici multipli nel gruppo di volumi il nome (**lv_name**) nella risorsa **lvm** deve restare vuoto o non specificato. Da notare anche che in una configurazione HA-LVM un gruppo di volumi può essere usato solo da un servizio.

4. Modificare il campo **volume_list** nel file **/etc/lvm/lvm.conf**. Includere il nome del gruppo di volumi root e l'hostname come riportato nel file **/etc/cluster/cluster.conf** preceduto da @. L'hostname da usare è la macchina sulla quale state modificando il file **lvm.conf**, e non un hostname remoto. Da notare che la stringa *DEVE* corrispondere al nome del nodo presente nel file **cluster.conf**. Di seguito viene riportata una voce d'esempio del file **/etc/lvm/lvm.conf**:

   ```
   volume_list = [ "VolGroup00", "@neo-01" ]
   ```

   Questo tag verrà usato per attivare VG o LV condivisi. *NON* includere i nomi di qualsiasi gruppo di volumi da condividere usando HA-LVM.

5. Aggiornare il dispositivo **initrd** su tutti i nodi del cluster:

   ```
   # dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
   ```

6. Riavviare tutti i nodi per usare il dispositivo **initrd** corretto.

APPENDICE G. DIARIO DELLE REVISIONI

Revisione 5.0-25.2.400 **2013-10-31** **Rüdiger Landmann**
Rebuild with publican 4.0.0

Revisione 5.0-25.2 **Thu May 2 2013** **Francesco Valente**
Italian translation completed

Revisione 5.0-25.1 **Thu Apr 18 2013** **Chester Cheng**
I file della traduzione sono sincronizzati con con le versioni 5.0-25 dei sorgenti XML

Revisione 5.0-25 **Mon Feb 18 2013** **Steven Levine**
Versione per la release 6.4 GA

Revisione 5.0-23 **Wed Jan 30 2013** **Steven Levine**
Resolve: 901641
Corregge le regole iptables.

Revisione 5.0-22 **Tue Jan 29 2013** **Steven Levine**
Resolve: 788636
Documenta la configurazione RRP attraverso il comando `ccs`.

Resolve: 789010
Documenta la configurazione RRP nel file `cluster.conf`.

Revisione 5.0-20 **Fri Jan 18 2013** **Steven Levine**
Resolve: 894097
Rimuove l'avviso per non utilizzare una associazione del tag VLAN.

Resolve: 845365
Indica che le modalità per il bonding 0 e 2 sono ora supportate.

Revisione 5.0-19 **Thu Jan 17 2013** **Steven Levine**
Resolve: 896234
Rende più chiara la terminologia per i riferimenti sui nodi del cluster.

Revisione 5.0-16 **Mon Nov 26 2012** **Steven Levine**
Versione per la release 6.4 Beta

Revisione 5.0-15 **Wed Nov 20 2012** **Steven Levine**

Resolve: 838988
Documenta l'attributo nfsrestart per gli agenti delle risorse del file system.

Resolve: 843169
Documenta il fencing agent IBM iPDU.

Resolve: 846121
Documenta l'agente per il fencing Eaton Network Power Controller (Interfaccia SNMP).

Resolve: 856834
Documenta l'agente per il fencing HP Bladesystem.

Resolve: 865313
Documenta l'agente delle risorse NFS Server.

Resolve: 862281
Specifica quale comando **`ccs`** sovrascrive le impostazioni precedenti.

Resolve: 846205
Documenta il processo di filtraggio del firewall **`iptables`** per il componente **`igmp`**.

Resolve: 857172
Documenta la possibilità di rimuovere gli utenti da luci.

Resolve: 857165
Documenta il parametro per il livello dei privilegi dell'agente di fencing IPMI.

Resolve: 840912
Risolve la problematica sulla formattazione con la tabella dei parametri delle risorse.

Resolve: 849240, 870292
Chiarisce la procedura di installazione.

Resolve: 871165
Chiarisce la descrizione del parametro dell'indirizzo IP nella descrizione dell'agente delle risorse per l'indirizzo stesso.

Resolve: 845333, 869039, 856681
Corregge piccoli errori di battitura e chiarisce alcune fasi tecniche.

Revisione 5.0-12 **Thu Nov 1 2012** **Steven Levine**
Aggiunti nuovi agenti per il fencing supportati.

Revisione 5.0-7 **Thu Oct 25 2012** **Steven Levine**
Aggiunta una sezione sulla sovrascrittura delle semantiche

Revisione 5.0-6 **Tue Oct 23 2012** **Steven Levine**
Corretto il valore predefinito di Post Join Delay.

Revisione 5.0-4 **Tue Oct 16 2012** **Steven Levine**
Aggiunta una descrizione sulla risorsa del server NFS.

Revisione 5.0-2 **Thu Oct 11 2012** **Steven Levine**
Aggiornamenti delle descrizioni di Conga.

Revisione 5.0-1 **Mon Oct 8 2012** **Steven Levine**
Chiarite le semantiche ccs

Revisione 4.0-5 **Fri Jun 15 2012** **Steven Levine**

Versione per la release 6.3 GA

Revisione 4.0-4 **Tue Jun 12 2012** **Steven Levine**

Resolve: 830148

Assicura uniformità negli esempi dei numeri di porte per luci.

Revisione 4.0-3 **Tue May 21 2012** **Steven Levine**

Resolve: 696897

Aggiunge le informazioni relative al parametro cluster.conf alle tabelle dei parametri del dispositivo di fence e delle risorse.

Risolve: 811643

Aggiunge un procedura per il ripristino di un database di **luci** su di una macchina separata.

Revisione 4.0-2 **Wed Apr 25 2012** **Steven Levine**

Risolve: 815619

Rimuove il messaggio di avvertimenti sull'uso di UDP Unicast con i file system GFS2.

Revisione 4.0-1 **Fri Mar 30 2012** **Steven Levine**

Risolve: 771447, 800069, 800061

Aggiorna la documentazione di **luci** per uniformarla con la versione Red Hat Enterprise Linux 6.3.

Risolve: 712393

Aggiunge le informzioni sulla cattura di un application core per RGManager.

Risolve: 800074

Documenta l'agente delle risorse `condor`.

Risolve: 757904

Documenta il ripristino e la configurazione del backup di **luci**.

Risolve: 772374

Aggiunge una sezione sulla gestione delle macchine virtuali in un cluster.

Risolve: 712378

Aggiunge la documentazione per la configurazione HA-LVM.

Risolve: 712400

Documenta le opzioni di debug.

Risolve: 751156

Documenta il nuovo parametro `fence_ipmilan`.

Risolve: 721373

Documenta le modifiche della configurazione che necessitano un riavvio del cluster.

Revisione 3.0-5 **Thu Dec 1 2011** **Steven Levine**

Release per il GA di Red Hat Enterprise Linux 6.2

Risolve: 755849

Corregge l'esempio del parametro monitor_link.

Revisione 3.0-4 **Mon Nov 7 2011** **Steven Levine**

Risolve: 749857

Aggiunge una documentazione per il dispositivo di fence RHEV-M REST API.

Revisione 3.0-3 **Fri Oct 21 2011** **Steven Levine**

Risolve: #747181, #747182, #747184, #747185, #747186, #747187, #747188, #747189, #747190, #747192
Corregge gli errori di battitura ed i passaggi poco chiari della documentazione riportati nel processo di revisione QE per Red Hat Enterprise Linux 6.2.

Revisione 3.0-2 **Fri Oct 7 2011** **Steven Levine**

Risolve: #743757
Corregge il riferimento alla modalità di bonding supportata nella sezione del troubleshooting.

Revisione 3.0-1 **Wed Sep 28 2011** **Steven Levine**

Versione iniziale della release Red Hat Enterprise Linux 6.2 Beta

Risolve: #739613
Documenta il supporto per le nuove opzioni **`ccs`** per la visualizzazione dei dispositivi di fence e dei servizi disponibili.

Risolve: #707740
Documenta gli aggiornamenti per l'interfaccia di Conga ed il supporto per l'impostazione dei permessi dell'utente per amministrare Conga.

Risolve: #731856
Documenta il supporto per la configurazione di **luci** tramite il file **`/etc/sysconfig/luci`**.

Risolve: #736134
Documenta il supporto per il trasporto UDPU.

Risolve: #736143
Documenta il supporto per il Samba clusterizzato.

Risolve: #617634
Documenta come configurare l'unico indirizzo IP al quale è servito **luci**.

Risolve: #713259
Documenta il supporto per l'agente **`fence_vmware_soap`**.

Risolve: #721009
Fornisce il link per l'articolo Support Essentials.

Risolve: #717006
Fornisce le informazioni sul traffico multicast attraverso il firewall **`iptables`**.

Risolve: #717008
Fornisce le informazioni sul controllo dello stato dei servizi del cluster e sul timeout del failover.

Risolve: #711868
Chiarisce la descrizione di autostart.

Risolve: #728337
Documenta la procedura su come aggiungere le risorse **`vm`** con il comando **`ccs`**.

Risolve: #725315, #733011, #733074, #733689
Corregge piccoli errori di battitura.

Revisione 2.0-1 **Thu May 19 2011** **Steven Levine**

Revisione iniziale di Red Hat Enterprise Linux 6.1

Risolve: #671250
Documenta il supporto per SNMP trap.

Risolve: #659753
Documenta il comando **`ccs`**.

Risolve: #665055
Aggiorna la documentazione di Conga in modo da riflettere il supporto aggiornato delle funzioni e del display.

Risolve: #680294
Documenta la necessità di un accesso con password per l'agente **`ricci`**.

Risolve: #687871
Aggiunge un capitolo al troubleshooting.

Risolve: #673217
Corregge gli errori di battitura

Risolve: #675805
Aggiunge il riferimento allo schema di **`cluster.conf`** alle tabelle dei parametri delle risorse HA.

Risolve: #672697
Aggiorna le tabelle dei parametri del dispositivo di fencing in modo da includere tutti i dispositivi attualmente supportati.

Risolve: #677994
Corregge le informazioni per i parametri dell'agente **`fence_ilo`**.

Risolve: #629471
Aggiunge le note tecniche sull'impostazione del valore di consensus in un cluster a due nodi.

Risolve: #579585
Aggiorna la sezione relativa all'aggiornamento del software Red Hat High Availability Add-On.

Risolve: #643216
Chiarisce le piccole problematiche presenti nel documento.

Risolve: #643191
Fornisce i miglioramenti e le correzioni per la documentazione di **luci**.

Risolve: #704539
Aggiorna la tabella dei parametri delle risorse della macchina virtuale.

Revisione 1.0-1 **Wed Nov 10 2010** **Paul Kennedy**
Release iniziale per Red Hat Enterprise Linux 6

INDICE ANALITICO

A

C

D

F

G

H

I

L

M

N

P

Q

R