

Red Hat Enterprise Linux 6

Cluster-Administration

Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons

Ausgabe 0



Rechtlicher Hinweis

Copyright © 2011 Red Hat Inc..

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at <http://creativecommons.org/licenses/by-sa/3.0/>. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

All other trademarks are the property of their respective owners.

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

Zusammenfassung

Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons beschreibt die Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons für Red Hat Enterprise Linux 6.

Inhaltsverzeichnis

Einführung

1. Dokumentkonventionen
 - 1.1. Typografische Konventionen
 - 1.2. Konventionen für Seitenansprachen (engl.: pull-quotes)
 - 1.3. Anmerkungen und Warnungen
 2. Feedback
1. Überblick über Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons
 - 1.1. Neue und veränderte Features für Red Hat Enterprise Linux 6.1
 - 1.2. Konfigurationsgrundlagen
 - 1.3. Einrichten der Hardware
 - 1.4. Installation der Red Hat Hochverfügbarkeits-Add-On-Software
 - 1.5. Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software
 2. Vor der Konfiguration des Hochverfügbarkeits-Add-Ons
 - 2.1. Allgemeine Überlegungen zur Konfiguration
 - 2.2. Kompatible Hardware
 - 2.3. Aktivieren von IP-Ports
 - 2.3.1. Aktivieren von IP-Ports auf Cluster-Knoten
 - 2.3.2. Aktivieren von IP-Ports auf Computern, die luci ausführen
 - 2.4. Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten
 - 2.4.1. Deaktivieren von ACPI Soft-Off mit dem `chkconfig`-Befehl
 - 2.4.2. Deaktivieren von ACPI Soft-Off im BIOS
 - 2.4.3. Vollständiges Deaktivieren von ACPI in der `grub.conf`-Datei
 - 2.5. Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten
 - 2.6. Überprüfung der Konfiguration
 - 2.7. Überlegungen zum NetworkManager
 - 2.8. Überlegungen zur Verwendung von Quorum Disk
 - 2.9. Red Hat Hochverfügbarkeits-Add-On und SELinux
 - 2.10. Multicast-Adressen
 - 2.11. Überlegungen zu `ricci`
 3. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga
 - 3.1. Konfigurationsaufgaben
 - 3.2. Starten von luci
 - 3.3. Erstellen eines Clusters
 - 3.4. Globale Cluster-Eigenschaften
 - 3.4.1. Konfiguration der allgemeinen Eigenschaften
 - 3.4.2. Konfiguration der Fencing-Geräteeigenschaften
 - 3.4.3. Netzwerkkonfiguration
 - 3.4.4. Quorum-Plattenkonfiguration
 - 3.4.5. Konfiguration der Protokollierung
 - 3.5. Konfiguration von Fencing-Geräten
 - 3.5.1. Erstellen eines Fencing-Geräts
 - 3.5.2. Ändern eines Fencing-Geräts
 - 3.5.3. Löschen eines Fencing-Geräts
 - 3.6. Konfiguration des Fencing für Cluster-Mitglieder
 - 3.6.1. Konfiguration eines einzelnen Fencing-Geräts für einen Knoten
 - 3.6.2. Konfiguration eines Backup-Fencing-Geräts
 - 3.6.3. Konfiguration eines Knotens mit redundanter Stromversorgung
 - 3.7. Konfiguration einer Ausfallsicherungs-Domain
 - 3.7.1. Hinzufügen einer Ausfallsicherungs-Domain
 - 3.7.2. Ändern einer Ausfallsicherungs-Domain

- 3.7.3. Löschen einer Ausfallsicherungs-Domain
- 3.8. Konfiguration von globalen Cluster-Eigenschaften
- 3.9. Hinzufügen eines Cluster-Dienstes zum Cluster
- 4. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga
 - 4.1. Hinzufügen eines vorhandenen Clusters zur Luci-Oberfläche
 - 4.2. Verwaltung von Cluster-Knoten
 - 4.2.1. Einen Cluster-Knoten neu starten
 - 4.2.2. Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen
 - 4.2.3. Ein Mitglied zu einem laufenden Cluster hinzufügen
 - 4.2.4. Ein Mitglied aus einem Cluster löschen
 - 4.3. Starten, Stoppen, Neustarten und Löschen von Clustern
 - 4.4. Verwaltung von Hochverfügbarkeitsdiensten
- 5. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem ccs-Befehl
 - 5.1. Überblick über operationale Aspekte
 - 5.1.1. Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System
 - 5.1.2. Anzeigen der aktuellen Cluster-Konfiguration
 - 5.1.3. Angeben des ricci-Passworts mit dem ccs-Befehl
 - 5.1.4. Ändern von Cluster-Konfigurationskomponenten
 - 5.2. Konfigurationsaufgaben
 - 5.3. Starten von ricci
 - 5.4. Erstellen eines Clusters
 - 5.5. Konfigurieren von Fencing-Geräten
 - 5.6. Konfigurieren von Fencing-Geräten für Cluster-Mitglieder
 - 5.6.1. Konfiguration eines einzelnen Power-Fencing-Geräts für einen Knoten
 - 5.6.2. Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten
 - 5.6.3. Konfiguration eines Backup-Fencing-Geräts
 - 5.6.4. Konfiguration eines Knotens mit redundanter Stromversorgung
 - 5.6.5. Entfernen von Fencing-Methoden und Fencing-Instanzen
 - 5.7. Konfigurieren einer Ausfallsicherungs-Domain
 - 5.8. Konfigurieren von globalen Cluster-Ressourcen
 - 5.9. Hinzufügen eines Cluster-Dienstes zum Cluster
 - 5.10. Konfigurieren einer Quorum-Platte
 - 5.11. Sonstige Cluster-Konfiguration
 - 5.11.1. Cluster-Konfigurationsversion
 - 5.11.2. Multicast-Konfiguration
 - 5.11.3. Konfiguration eines Zwei-Knoten-Clusters
 - 5.12. Verbreiten der Konfigurationsdatei auf den Cluster-Knoten
- 6. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit ccs
 - 6.1. Verwaltung von Cluster-Knoten
 - 6.1.1. Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen
 - 6.1.2. Ein Mitglied zu einem laufenden Cluster hinzufügen
 - 6.2. Starten und Stoppen eines Clusters
 - 6.3. Fehlerdiagnose und -behebung in einem Cluster
- 7. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools
 - 7.1. Konfigurationsaufgaben
 - 7.2. Erstellen einer einfachen Cluster-Konfigurationsdatei
 - 7.3. Konfiguration von Fencing
 - 7.4. Konfiguration von Ausfallsicherungs-Domains
 - 7.5. Konfiguration von Hochverfügbarkeitsdiensten
 - 7.5.1. Hinzufügen von Cluster-Ressourcen
 - 7.5.2. Hinzufügen eines Cluster-Dienstes zum Cluster
 - 7.6. Überprüfen der Konfiguration

8. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools

8.1. Starten und Stoppen der Cluster-Software

8.1.1. Starten der Cluster-Software

8.1.2. Stoppen der Cluster-Software

8.2. Hinzufügen oder Löschen eines Knotens

8.2.1. Einen Knoten vom Cluster löschen

8.2.2. Einen Knoten zum Cluster hinzufügen

8.2.3. Beispiele für Drei-Knoten- und Zwei-Knoten-Konfigurationen

8.3. Verwaltung von Hochverfügbarkeitsdiensten

8.3.1. Anzeige des Hochverfügbarkeitsdienst-Status mit `clustat`

8.3.2. Verwaltung von Hochverfügbarkeitsdiensten mit `clusvcadm`

8.4. Aktualisieren einer Konfiguration

8.4.1. Aktualisieren der Konfiguration mittels `cman_tool version -r`

8.4.2. Aktualisieren der Konfiguration mittels `scp`

9. Fehlerdiagnose und -behebung in einem Cluster

9.1. Cluster wird nicht gebildet

9.2. Knoten können nach Fencing oder Neustart dem Cluster nicht wieder beitreten

9.3. Cluster-Dienste hängen sich auf

9.4. Cluster-Dienst startet nicht

9.5. Migration von Cluster-verwalteten Diensten schlägt fehl

9.6. Jeder Knoten in einem Zwei-Knoten-Cluster meldet den jeweils anderen Knoten als ausgefallen

9.7. Knoten werden nach LUN-Pfad-Ausfall abgegrenzt

9.8. Quorum-Platte erscheint nicht als Cluster-Mitglied

9.9. Ungewöhnliches Verhalten bei Ausfallsicherung

9.10. Wahlloses Fencing

10. SNMP-Konfiguration mit dem Red Hat Hochverfügbarkeits-Add-On

10.1. SNMP und das Red Hat Hochverfügbarkeits-Add-On

10.2. Konfiguration von SNMP mit dem Red Hat Hochverfügbarkeits-Add-On

10.3. Weiterleiten von SNMP-Traps

10.4. SNMP-Traps generiert vom Red Hat Hochverfügbarkeits-Add-On

A. Parameter der Fencing-Geräte

B. Parameter der Hochverfügbarkeitsressourcen

C. Verhalten der Hochverfügbarkeitsressourcen

C.1. Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen

C.2. Startreihenfolge von Kind- und Geschwisterressourcen

C.2.1. Start-/Stopp-Reihenfolge von typisierten Kindressourcen

C.2.2. Start- und Stoppreihenfolge von nicht typisierten Kindressourcen

C.3. Vererbung, der `<resources>`-Block, und Wiederverwendung von Ressourcen

C.4. Wiederherstellung nach Ausfall und Unabhängige Unterbäume

C.5. Testen und Fehlerbehebung von Diensten und der Ressourcenreihenfolge

D. Überblick über Befehlszeilen-Tools

E. Versionsgeschichte

Stichwortverzeichnis

Einführung

Dieses Handbuch liefert Informationen zur Installation, Konfiguration und Verwaltung der Komponenten des Red Hat Hochverfügbarkeits-Add-Ons. Die Komponenten des Red Hat Hochverfügbarkeits-Add-Ons erlauben Ihnen das Verbinden einer Gruppe von Computern (genannt *Knoten* oder *Mitglieder*), um als Cluster zusammenzuarbeiten. In diesem Dokument bezieht sich das Wort *Cluster* auf eine Gruppe von Computern, auf denen das Red Hat Hochverfügbarkeits-Add-On läuft.

Die Zielgruppe dieses Handbuchs sollte bereits über umfassende Kenntnisse von Red Hat Enterprise Linux verfügen und die Konzepte von Clustern, Speicher und Server-Rechnern verstehen.

Dieses Dokument ist folgendermaßen aufgebaut:

- ▶ [Kapitel 1, Überblick über Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons](#)
- ▶ [Kapitel 2, Vor der Konfiguration des Hochverfügbarkeits-Add-Ons](#)
- ▶ [Kapitel 3, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#)
- ▶ [Kapitel 4, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#)
- ▶ [Kapitel 7, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#)
- ▶ [Kapitel 8, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#)
- ▶ [Kapitel 9, Fehlerdiagnose und -behebung in einem Cluster](#)
- ▶ [Kapitel 10, SNMP-Konfiguration mit dem Red Hat Hochverfügbarkeits-Add-On](#)
- ▶ [Anhang A, Parameter der Fencing-Geräte](#)
- ▶ [Anhang B, Parameter der Hochverfügbarkeitsressourcen](#)
- ▶ [Anhang C, Verhalten der Hochverfügbarkeitsressourcen](#)
- ▶ [Anhang D, Überblick über Befehlszeilen-Tools](#)
- ▶ [Anhang E, Versionsgeschichte](#)

Werfen Sie einen Blick auf die folgenden Quellen für weitere Informationen über Red Hat Enterprise Linux 6.

- ▶ *Red Hat Enterprise Linux Installationshandbuch* — Liefert Informationen bezüglich der Installation von Red Hat Enterprise Linux 6.
- ▶ *Red Hat Enterprise Linux Deployment-Handbuch* — Liefert Informationen bezüglich der Implementierung, der Konfiguration und der Administration von Red Hat Enterprise Linux 6.

Werfen Sie einen Blick auf die folgenden Quellen für weitere Informationen über das Hochverfügbarkeits-Add-On und zugehörige Produkte für Red Hat Enterprise Linux 6:

- ▶ *Überblick über das Hochverfügbarkeits-Add-On* — Liefert einen umfassenden Überblick über das Red Hat Hochverfügbarkeits-Add-On.
- ▶ *Administration des Logical Volume Manager* — Liefert eine Beschreibung des Logical Volume Managers (LVM), inklusive Informationen zum Einsatz von LVM in einer Cluster-Umgebung.
- ▶ *Global File System 2: Konfiguration und Administration* — Liefert Informationen zur Installation, Konfiguration und Pflege von Red Hat GFS (Red Hat Global File System 2), das Bestandteil des Resilient-Storage-Add-Ons ist.
- ▶ *DM Multipath* — Liefert Informationen über die Verwendung des Device-Mapper Multipath Features von Red Hat Enterprise Linux 6.
- ▶ *Lastverteilungs-Administration* — Liefert Informationen zur Konfiguration von Hochleistungssystemen und -diensten mit dem Red Hat Lastverteilungs-Add-On, einer Gruppe integrierter Software-Komponenten, die Linux Virtual Server (LVS) bereitstellen, um IP-Lasten über eine Gruppe realer Server zu verteilen.
- ▶ *Versionshinweise* — Liefert Informationen zu aktuellen Releases von Red Hat Produkten.

Diese und weitere Red Hat Handbücher stehen als HTML-, PDF- und RPM-Versionen auf der Red Hat Enterprise Linux-Dokumentations-CD und online unter <http://docs.redhat.com/> zur Verfügung.

1. Dokumentkonventionen

Dieses Handbuch verwendet mehrere Konventionen, um bestimmte Wörter und Phrasen hervorzuheben und Aufmerksamkeit auf spezifische Informationen zu lenken.

In PDF- und Papierausgaben verwendet dieses Handbuch Schriftbilder des [Liberation-Fonts](#)-Sets. Das Liberation-Fonts-Set wird auch für HTML-Ausgaben verwendet, falls es auf Ihrem System installiert ist. Falls nicht, werden alternative, aber äquivalente Schriftbilder angezeigt. Beachten Sie: Red Hat Enterprise Linux 5 und die nachfolgende Versionen beinhalten das Liberation-Fonts-Set standardmäßig.

1.1. Typografische Konventionen

Es werden vier typografische Konventionen verwendet, um die Aufmerksamkeit auf spezifische Wörter und Phrasen zu lenken. Diese Konventionen und die Umstände, unter denen sie auftreten, sind folgende:

Nichtproportional Fett

Dies wird verwendet, um Systemeingaben hervorzuheben, einschließlich Shell-Befehle, Dateinamen und Pfade. Es wird ebenfalls zum Hervorheben von Tasten und Tastenkombinationen verwendet. Zum Beispiel:

Um den Inhalt der Datei `my_next_bestselling_novel` in Ihrem aktuellen Arbeitsverzeichnis zu sehen, geben Sie den Befehl `cat my_next_bestselling_novel` in den Shell-Prompt ein und drücken Sie **Enter**, um den Befehl auszuführen.

Das oben aufgeführte Beispiel beinhaltet einen Dateinamen, einen Shell-Befehl und eine Taste. Alle werden nichtproportional fett dargestellt und alle können, dank des Kontextes, leicht unterschieden werden.

Die Tastenkombination kann von einer Taste durch ein Pluszeichen, das alle Teile der Tastenkombination miteinander verbindet, unterschieden werden. Zum Beispiel:

Drücken Sie **Enter**, um den Befehl auszuführen.

Press **Ctrl+Alt+F2** to switch to a virtual terminal.

Der erste Absatz hebt die jeweilige Taste hervor, die gedrückt werden soll. Der zweite Absatz hebt zwei Tastenkombinationen hervor (jeweils ein Satz von drei Tasten, wobei jeder Satz gleichzeitig gedrückt wird).

Falls Quellcode diskutiert wird, werden Klassennamen, Methoden, Funktionen, Variablennamen und Rückgabewerte, die innerhalb eines Abschnitts erwähnt werden, wie oben gezeigt **nichtproportional fett** dargestellt. Zum Beispiel:

Zu dateiverwandten Klassen zählen **filesystem** für Dateisysteme, **file** für Dateien und **dir** für Verzeichnisse. Jede Klasse hat ihren eigenen Satz an Berechtigungen.

Proportional Fett

Dies kennzeichnet Wörter oder Phrasen, die auf einem System vorkommen, einschließlich Applikationsnamen, Text in Dialogboxen, beschriftete Schaltflächen, Bezeichnungen für Auswahlkästchen und Radio-Buttons, Überschriften von Menüs und Untermenüs. Zum Beispiel:

Wählen Sie **System** → **Einstellungen** → **Maus** in der Hauptmenüleiste aus, um die **Mauseinstellungen** zu öffnen. Klicken Sie im Reiter **Tasten** auf das Auswahlkästchen **Mit links bediente Maus** und anschließend auf **Schließen**, um die primäre Maustaste von der linken auf die rechte Seite zu ändern (d.h., um die Maus auf Linkshänder anzupassen).

To insert a special character into a **gedit** file, choose **Applications** → **Accessories** → **Character Map** from the main menu bar. Next, choose **Search** → **Find...** from the **Character Map** menu bar, type the name of the character in the **Search** field and click

Next. The character you sought will be highlighted in the **Character Table**. Double-click this highlighted character to place it in the **Text to copy** field and then click the **Copy** button. Now switch back to your document and choose **Edit** → **Paste** from the **gedit** menu bar.

Der oben aufgeführte Text enthält Applikationsnamen, systemweite Menünamen und -elemente, applikationsspezifische Menünamen sowie Schaltflächen und Text innerhalb einer GUI-Oberfläche. Alle werden proportional fett dargestellt und sind anhand des Kontextes unterscheidbar.

Nichtproportional Fett Kursiv oder ***Proportional Fett Kursiv***

Egal ob nichtproportional fett oder proportional fett, ein zusätzlicher Kursivdruck weist auf einen ersetzbaren oder variablen Text hin. Kursivdruck kennzeichnet Text, der nicht wörtlich eingegeben wird, oder angezeigter Text, der sich je nach gegebenen Umständen ändert. Zum Beispiel:

Um sich mit einer Remote-Maschine via SSH zu verbinden, geben Sie an einem Shell-Prompt **ssh *username@domain.name*** ein. Falls die Remote-Maschine **example.com** ist und Ihr Benutzername auf dieser Maschine John lautet, geben Sie also **ssh *john@example.com*** ein.

Der Befehl **mount -o remount *file-system*** hängt das angegebene Dateisystem wieder ein. Um beispielsweise das **/home**-Dateisystem wieder einzuhängen, verwenden Sie den Befehl **mount -o remount /home**.

Um die Version des derzeit installierten Pakets zu sehen, verwenden Sie den Befehl **rpm -q *package***. Die Ausgabe sieht wie folgt aus: ***package-version-release***.

Note the words in bold italics above — *username*, *domain.name*, *file-system*, *package*, *version* and *release*. Each word is a placeholder, either for text you enter when issuing a command or for text displayed by the system.

Neben der Standardbenutzung für die Darstellung des Titels eines Werks, zeigt der Kursivdruck auch die erstmalige Nutzung eines neuen und wichtigen Begriffs an. Zum Beispiel:

Publican ist ein *DocBook* Publishing-System.

1.2. Konventionen für Seitenansprachen (engl.: pull-quotes)

Ausgaben des Terminals und Auszüge aus dem Quellcode werden visuell vom umliegenden Text hervorgehoben.

Eine Ausgabe, die an das Terminal gesendet wird, wird in den Schrifttyp **nichtproportional Roman** gesetzt und demnach wie folgt präsentiert:

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

Auszüge aus dem Quellcode werden ebenfalls in den Schrifttyp **nichtproportional Roman** gesetzt, doch wird zusätzlich noch die Syntax hervorgehoben:

```

package org.jboss.book.jca.ex1;

import javax.naming.InitialContext;

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

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

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

```

1.3. Anmerkungen und Warnungen

Zu guter Letzt verwenden wir drei visuelle Stile, um die Aufmerksamkeit auf Informationen zu lenken, die andernfalls vielleicht übersehen werden könnten.



Anmerkung

Eine Anmerkung ist ein Tipp, ein abgekürztes Verfahren oder ein alternativer Ansatz für die vorliegende Aufgabe. Das Ignorieren von Anmerkungen sollte keine negativen Auswirkungen haben, aber Sie verpassen so vielleicht einen Trick, der Ihnen das Leben vereinfachen könnte.



Wichtig

Die Wichtig-Schaukästen lenken die Aufmerksamkeit auf Dinge, die sonst leicht übersehen werden können: Konfigurationsänderungen, die nur für die aktuelle Sitzung gelten oder Dienste, für die ein Neustart nötig ist, bevor eine Aktualisierung wirksam wird. Das Ignorieren von Wichtig-Schaukästen würde keinen Datenverlust verursachen, kann aber unter Umständen zu Ärgernissen und Frustration führen.



Warnung

Eine Warnung sollte nicht ignoriert werden. Das Ignorieren von Warnungen führt mit hoher Wahrscheinlichkeit zu Datenverlust.

2. Feedback

Falls Sie einen Fehler in diesem Handbuch finden oder eine Idee haben, wie dieses verbessert werden könnte, freuen wir uns über Ihr Feedback! Bitte reichen Sie einen Fehlerbericht in Bugzilla (<http://bugzilla.redhat.com/bugzilla/>) für die Komponente **doc-Cluster_Administration** ein.

Vergewissern Sie sich beim Einreichen eines Fehlerberichts, dass Sie die Kennung des Handbuchs mit angeben:

Cluster_Administration(EN)-6 (2011-05-19T16:26)

Indem Sie die Kennung des Handbuchs angeben, wissen wir genau, welche Version des Handbuchs Sie

vorliegen haben.

Falls Sie uns einen Vorschlag zur Verbesserung der Dokumentation senden möchten, sollten Sie hierzu möglichst genaue Angaben machen. Wenn Sie einen Fehler gefunden haben, geben Sie bitte die Nummer des Abschnitts und einen Ausschnitt des Textes an, damit wir diesen leicht finden können.

Kapitel 1. Überblick über Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons

Das Red Hat Hochverfügbarkeits-Add-On erlaubt Ihnen das Verbinden einer Gruppe von Computern (genannt *Knoten* oder *Mitglieder*), um als Cluster zusammenzuarbeiten. Sie können das Red Hat Hochverfügbarkeits-Add-On auf Ihre Clustering-Bedürfnisse anpassen (z.B. zum Einrichten eines Clusters zur gemeinsamen Dateinutzung auf einem GFS2-Dateisystem oder zum Einrichten einer Dienstaussfallsicherung).

Dieses Kapitel liefert eine Zusammenfassung der Features und Aktualisierungen, die seit der ursprünglichen Release von Red Hat Enterprise Linux 6 zum Red Hat Hochverfügbarkeits-Add-On hinzugefügt wurden, gefolgt von einer Übersicht über die Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons.

1.1. Neue und veränderte Features für Red Hat Enterprise Linux 6.1

Red Hat Enterprise Linux 6.1 führt die folgenden Änderungen und Aktualisierungen an Dokumentationen und Features ein.

- ▶ Ab der Red Hat Enterprise Linux 6.1 Release bietet das Red Hat Hochverfügbarkeits-Add-On Unterstützung für SNMP-Traps. Informationen über die Konfiguration von SNMP-Traps mit dem Red Hat Hochverfügbarkeits-Add-On finden Sie in [Kapitel 10, SNMP-Konfiguration mit dem Red Hat Hochverfügbarkeits-Add-On](#).
- ▶ Ab der Red Hat Enterprise Linux 6.1 Release bietet das Red Hat Hochverfügbarkeits-Add-On Unterstützung für den `ccs`-Cluster-Konfigurationsbefehl. Informationen über den `ccs`-Befehl finden Sie in [Kapitel 5, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem `ccs`-Befehl](#) und [Kapitel 6, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit `ccs`](#).
- ▶ Die Dokumentation über die Konfiguration und Verwaltung der Red Hat Hochverfügbarkeits-Add-On-Software mittels Conga wurde aktualisiert, um aktuelle Conga-Bildschirme und unterstützte Features aufzunehmen.
- ▶ Für die Red Hat Enterprise Linux 6.1 Release und später ist für die Verwendung von `ricci` ein Passwort erforderlich, wenn Sie zum ersten Mal eine aktualisierte Cluster-Konfiguration von einem bestimmten Knoten verbreiten. Weitere Informationen über `ricci` finden Sie unter [Abschnitt 2.11, „Überlegungen zu `ricci`“](#).
- ▶ Sie können nun die `Restart-Disable` Wiederherstellungsrichtlinie für einen Dienst festlegen, wodurch das System einen Neustart des ausgefallenen Dienstes an demselben Standort versucht. Scheitert dieser Versuch, wird der Dienst deaktiviert, statt auf einen anderen Host im Cluster verlegt zu werden. Dieses Feature ist in [Abschnitt 3.9, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#) und [Anhang B, Parameter der Hochverfügbarkeitsressourcen](#) dokumentiert.
- ▶ Sie können nun einen unabhängigen Unterbaum als nicht-kritisch konfigurieren, so dass im Falle eines Ausfalls dieser Ressource nur diese Ressource deaktiviert wird (statt des gesamten Dienstes). Informationen über dieses Feature finden Sie in [Abschnitt 3.9, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#) und [Abschnitt C.4, „Wiederherstellung nach Ausfall und Unabhängige Unterbäume“](#).
- ▶ Dieses Dokument enthält nun das neue Kapitel [Kapitel 9, Fehlerdiagnose und -behebung in einem Cluster](#).

Zusätzlich wurden im gesamten Dokument kleinere Korrekturen vorgenommen und einige Sachverhalte verdeutlicht.

1.2. Konfigurationsgrundlagen

Um einen Cluster einzurichten, müssen Sie die Knoten an bestimmte Cluster-Hardware anschließen und die Knoten für die Cluster-Umgebung konfigurieren. Die Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons umfasst die folgenden, grundlegenden Schritte:

1. Einrichten der Hardware. Siehe [Abschnitt 1.3, „Einrichten der Hardware“](#).

2. Installation der Red Hat Hochverfügbarkeits-Add-On Software. Siehe [Abschnitt 1.4, „Installation der Red Hat Hochverfügbarkeits-Add-On-Software“](#).
3. Konfiguration der Red Hat Hochverfügbarkeits-Add-On Software. Siehe [Abschnitt 1.5, „Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software“](#).

1.3. Einrichten der Hardware

Zum Einrichten der Hardware gehört das Verbinden der Cluster-Knoten mit anderer Hardware, die zum Ausführen des Red Hat Hochverfügbarkeits-Add-Ons nötig ist. Der Umfang und die Art der Hardware richtet sich nach dem Zweck und den Ansprüchen an die Verfügbarkeit des Clusters. In der Regel erfordert ein Cluster auf Unternehmensebene die folgende Hardware (siehe [Abbildung 1.1, „Überblick über die Red Hat Hochverfügbarkeits-Add-On-Hardware“](#)). Werfen Sie für Hardware-Überlegungen und andere Themen der Cluster-Konfiguration einen Blick auf [Kapitel 2, Vor der Konfiguration des Hochverfügbarkeits-Add-Ons](#) oder setzen Sie sich mit einem autorisierten Red Hat Vertreter in Verbindung.

- ▶ Hochverfügbarkeits-Add-On-Knoten — Computer, die Red Hat Enterprise Linux 6 Software ausführen können, mit mindestens 1 GB RAM.
- ▶ Ethernet Switch oder Hub für öffentliches Netzwerk — Dies ist nötig für den Client-Zugriff auf den Cluster.
- ▶ Ethernet Switch oder Hub für privates Netzwerk — Dies ist nötig zur Kommunikation zwischen den Cluster-Knoten und anderer Cluster-Hardware wie z.B. Netzwerk-Netzschalter und Fibre Channel Switches.
- ▶ Netzwerk-Netzschalter — Ein Netzwerk-Netzschalter wird empfohlen, um in einem Cluster der Unternehmensklasse sog. "Fencing" (Datenabgrenzung) durchführen zu können.
- ▶ Fibre Channel Switch — Ein Fibre Channel Switch ermöglicht Zugriff auf Fibre-Channel-Speicher. Abhängig vom Speicher-Schnittstellentyp stehen auch andere Speicheroptionen zur Verfügung, z.B. iSCSI. Ein Fibre Channel Switch kann zum Durchführen von Fencing konfiguriert werden.
- ▶ Speicher — Für einen Cluster sind bestimmte Speichertypen notwendig. Der nötige Typ hängt vom Zweck des Clusters ab.

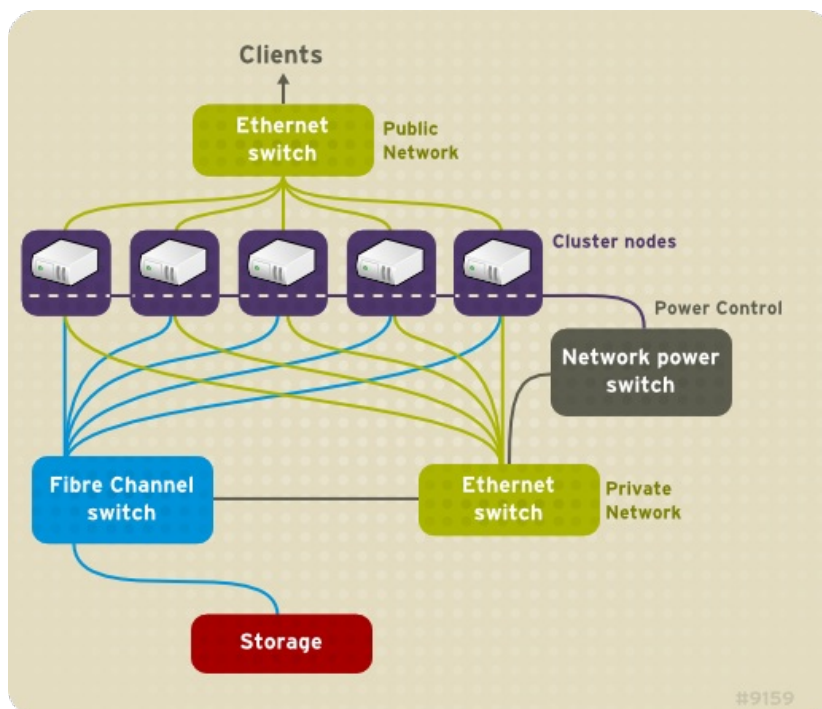


Abbildung 1.1. Überblick über die Red Hat Hochverfügbarkeits-Add-On-Hardware

1.4. Installation der Red Hat Hochverfügbarkeits-Add-On-Software

Um die Red Hat Hochverfügbarkeits-Add-On-Software zu installieren, benötigen Sie Berechtigungen für die Software. Falls Sie die **Conga**-Konfigurationsoberfläche verwenden, kann diese die Installation der Cluster-Software übernehmen. Falls Sie andere Tools zur Konfiguration des Clusters verwenden, sichern und installieren Sie die Software so, wie Sie dies mit jeder anderen Red Hat Enterprise Linux Software auch tun würden.

Aktualisieren der Red Hat Hochverfügbarkeits-Add-On-Software

Es ist möglich, die Cluster-Software auf eine beliebige Hauptversion von Red Hat Enterprise Linux zu aktualisieren, ohne den Cluster dafür außer Betrieb nehmen zu müssen. Dafür muss die Cluster-Software auf allen Hosts einzeln nacheinander deaktiviert, die Software aktualisiert und anschließend die Cluster-Software auf dem Host wieder gestartet werden.

1. Stoppen Sie sämtliche Cluster-Dienste auf einem einzelnen Cluster-Knoten. Eine Anleitung zum Stoppen der Cluster-Software auf einem Knoten finden Sie in [Abschnitt 8.1.2, „Stoppen der Cluster-Software“](#). Gegebenenfalls kann es von Vorteil sein, cluster-verwaltete Dienste und virtuelle Maschinen manuell vom Host zu verlegen, bevor **rgmanager** gestoppt wird.
2. Führen Sie **yum update** aus, um die neuen RPMs zu installieren. Zum Beispiel:

```
# yum update -y openais cman rgmanager lvm2-cluster gfs2-utils
```

3. Starten Sie den Cluster-Knoten neu oder führen Sie manuell einen Neustart der Cluster-Dienste aus. Eine Anleitung zum Starten der Cluster-Software auf einem Knoten finden Sie in [Abschnitt 8.1.1, „Starten der Cluster-Software“](#).

1.5. Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software

Zur Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software gehört die Verwendung von Konfigurations-Tools, um die Relationen der Cluster-Komponenten untereinander zu definieren. Die folgenden Cluster-Konfigurations-Tools stehen im Rahmen des Red Hat Hochverfügbarkeits-Add-Ons zur Verfügung:

- ▶ **Conga** — Hierbei handelt es sich um eine umfangreiche Benutzeroberfläche zur Installation, Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons. Werfen Sie einen Blick auf [Kapitel 3, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#) und [Kapitel 4, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#) für Informationen zur Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons mit **Conga**.
- ▶ Der **ccs**-Befehl — Dieser Befehl konfiguriert und verwaltet das Red Hat Hochverfügbarkeits-Add-On. Werfen Sie einen Blick auf [Kapitel 5, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem ccs-Befehl](#) und [Kapitel 6, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit ccs](#) für Informationen zur Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons mit dem **ccs**-Befehl.
- ▶ Befehlszeilen-Tools — Hierbei handelt es sich um eine Reihe Befehlszeilen-Tools zur Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons. Werfen Sie einen Blick auf [Kapitel 7, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#) und [Kapitel 8, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#) für Informationen zur Konfiguration und Verwaltung eines Clusters mit Kommandozeilen-Tools. Siehe [Anhang D, Überblick über Befehlszeilen-Tools](#) für eine Übersicht der bevorzugten Befehlszeilen-Tools.



Anmerkung

system-config-cluster steht in RHEL 6 nicht zur Verfügung.

Kapitel 2. Vor der Konfiguration des Hochverfügbarkeits-Add-Ons

Dieses Kapitel beschreibt die Aufgaben, die vor der Installation und Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons durchgeführt werden müssen. Es besteht aus den folgenden Abschnitten.



Wichtig

Stellen Sie sicher, dass Ihr Deployment des Red Hat Hochverfügbarkeits-Add-Ons Ihren Anforderungen gerecht wird und unterstützt werden kann. Beratschlagen Sie sich dazu ggf. mit einem autorisierten Red Hat Vertreter, um Ihre Konfiguration vor dem Deployment zu verifizieren. Berücksichtigen Sie zudem eine gewisse Zeit für einen Burn-In-Test, um die Konfiguration auf mögliche Ausfälle zu überprüfen.

- ▶ [Abschnitt 2.1, „Allgemeine Überlegungen zur Konfiguration“](#)
- ▶ [Abschnitt 2.2, „Kompatible Hardware“](#)
- ▶ [Abschnitt 2.3, „Aktivieren von IP-Ports“](#)
- ▶ [Abschnitt 2.4, „Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten“](#)
- ▶ [Abschnitt 2.5, „Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten“](#)
- ▶ [Abschnitt 2.6, „Überprüfung der Konfiguration“](#)
- ▶ [Abschnitt 2.7, „Überlegungen zum NetworkManager“](#)
- ▶ [Abschnitt 2.8, „Überlegungen zur Verwendung von Quorum Disk“](#)
- ▶ [Abschnitt 2.9, „Red Hat Hochverfügbarkeits-Add-On und SELinux“](#)
- ▶ [Abschnitt 2.10, „Multicast-Adressen“](#)
- ▶ [Abschnitt 2.11, „Überlegungen zu ricci“](#)

2.1. Allgemeine Überlegungen zur Konfiguration

Sie können das Red Hat Hochverfügbarkeits-Add-On auf vielerlei Arten konfigurieren, um Ihren Bedürfnissen gerecht zu werden. Berücksichtigen Sie beim Planen, Konfigurieren und Implementieren Ihres Deployments die folgenden, allgemeinen Überlegungen.

Anzahl der unterstützten Cluster-Knoten

Das Hochverfügbarkeits-Add-On unterstützt maximal 16 Cluster-Knoten.

Cluster an einem einzelnen Standort

Derzeit werden nur Cluster unterstützt, die sich an einem einzigen physischen Standort befinden. Cluster, die über mehrere physische Standorte verteilt sind, werden offiziell nicht unterstützt. Für weitere Einzelheiten und Informationen über Cluster an mehreren Standorten setzen Sie sich bitte mit Ihrem Red Hat Vertriebs- oder Kundendienstmitarbeiter in Verbindung.

GFS2

Obwohl das GFS2-Dateisystem sowohl auf einem eigenständigen System als auch als Teil einer Cluster-Konfiguration implementiert werden kann, unterstützt Red Hat den Einsatz von GFS2 nicht für ein Ein-Knoten-System. Red Hat unterstützt jedoch eine Reihe von leistungsstarken Ein-Knoten-Dateisystemen, die für den Einsatz auf einzelnen Knoten optimiert sind und dadurch meist einen geringeren Overhead als ein Cluster-Dateisystem haben. Red Hat empfiehlt den Einsatz eines dieser Dateisysteme anstelle von GFS2 in Fällen, in denen nur ein einzelner Knoten das Dateisystem einhängen muss. Red Hat wird für Bestandskunden weiterhin Ein-Knoten-GFS2-Dateisysteme unterstützen.

Wenn Sie ein GFS2-Dateisystem als ein Cluster-Dateisystem konfigurieren, müssen Sie

sicherstellen, dass alle Knoten im Cluster Zugriff auf das gemeinsame Dateisystem haben. Asymmetrische Cluster-Konfigurationen, bei denen einige Knoten Zugriff auf den Speicher haben und andere nicht, werden nicht unterstützt. Es ist jedoch nicht nötig, dass alle Knoten das GFS2-Dateisystem auch tatsächlich selbst einhängen.

Hardware-Konfiguration ohne einzelne Ausfallpunkte

Cluster können ein Dual-Controller RAID-Array, mehrere gebündelte Netzwerkkanäle, mehrere Pfade zwischen Cluster-Mitgliedern und Speicher sowie UPS-Systeme ("Un-interruptible Power Supply" oder unterbrechungsfreie Stromversorgung) umfassen, um sicherzustellen, dass kein einzelner Ausfallpunkt zu Datenverlust oder Ausfallzeiten der Applikationen führt.

Alternativ kann ein kostengünstiger Cluster eingerichtet werden, der eine geringere Verfügbarkeit als ein Cluster ohne einzelnen Ausfallpunkt bietet. Beispielsweise können Sie einen Cluster mit einem Single-Controller RAID-Array und einem einzelnen Ethernet-Kanal einrichten.

Einige kostengünstige Alternativen, wie z.B. Host RAID Controller, Software RAID ohne Clustering-Unterstützung und parallele Multi-Initiator-SCSI-Konfigurationen sind nicht kompatibel bzw. nicht geeignet für den Einsatz als gemeinsam verwendeter Cluster-Speicher.

Gewährleistung der Datenintegrität

Um die Datenintegrität zu gewährleisten, darf zu jeder Zeit nur ein Knoten einen Cluster-Dienst ausführen und auf die zugehörigen Daten zugreifen. Mithilfe von Netzschaltern in der Cluster-Hardware-Konfiguration kann bei einem Ausfall ein Knoten einen anderen Knoten aus- und wieder einschalten, bevor dessen Hochverfügbarkeitsdienste neu gestartet werden. Dadurch wird verhindert, dass zwei Knoten gleichzeitig auf dieselben Daten zugreifen und diese dadurch beschädigen. Es wird dringend empfohlen, *Fencing-Geräte* (Hardware- oder Software-Lösungen, die von Remote aus Cluster-Knoten aus- und anschalten und neu starten können) einzusetzen, um selbst im Falle eines Ausfalls die Datenintegrität gewährleisten zu können.

Ethernet-Kanalbündelung

Das Cluster-Quorum und die Knoten-Zustände werden anhand von Meldungen bestimmt, die via Ethernet zwischen den Cluster-Knoten übertragen werden. Die Cluster-Knoten nutzen das Ethernet darüber hinaus für eine Vielzahl anderer kritischer Cluster-Funktionen (z.B. das Fencing). Bei der Ethernet-Kanalbündelung werden mehrere Ethernet-Schnittstellen so konfiguriert, dass diese sich wie eine einzige Schnittstelle verhalten, wodurch das Risiko eines einzelnen Ausfallpunktes in der herkömmlichen Ethernet-Verbindung zwischen Cluster-Knoten und anderer Cluster-Hardware vermieden wird.

IPv4 und IPv6

Das Hochverfügbarkeits-Add-On unterstützt sowohl das IPv4- als auch das IPv6-Internetprotokoll. Die Unterstützung für IPv6 im Hochverfügbarkeits-Add-On ist neu für Red Hat Enterprise Linux 6.

2.2. Kompatible Hardware

Vergewissern Sie sich vor der Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software, dass Ihr Cluster geeignete Hardware verwendet (z.B. unterstützte Fencing-Geräte, Speichergeräte und Fibre Channel Switches). Werfen Sie einen Blick auf die Richtlinien zur Hardware-Konfiguration unter http://www.redhat.com/cluster_suite/hardware/ für die aktuellsten Informationen über kompatible Hardware.

2.3. Aktivieren von IP-Ports

Vor dem Einsatz des Red Hat Hochverfügbarkeits-Add-Ons müssen Sie bestimmte IP-Ports auf den Cluster-Knoten und auf Computern, die **luci** (den Server für die **Conga**-Benutzeroberfläche) ausführen, aktivieren. Die folgenden Abschnitte zeigen die IP-Ports auf, die aktiviert werden müssen:

- ▶ [Abschnitt 2.3.1, „Aktivieren von IP-Ports auf Cluster-Knoten“](#)
- ▶ [Abschnitt 2.3.2, „Aktivieren von IP-Ports auf Computern, die **luci** ausführen“](#)

2.3.1. Aktivieren von IP-Ports auf Cluster-Knoten

Um den Knoten des Red Hat Hochverfügbarkeits-Add-Ons die Kommunikation untereinander zu ermöglichen, müssen Sie die IP-Ports aktivieren, die zu bestimmten Komponenten des Red Hat Hochverfügbarkeits-Add-Ons gehören. [Tabelle 2.1, „Aktivierte IP-Ports auf Red Hat Hochverfügbarkeits-Add-On Knoten“](#) listet die IP-Port-Nummern, ihre zugehörigen Protokolle und die den Port-Nummern zugehörigen Komponenten auf. Aktivieren Sie auf jedem Cluster-Knoten die IP-Ports gemäß [Tabelle 2.1, „Aktivierte IP-Ports auf Red Hat Hochverfügbarkeits-Add-On Knoten“](#). Sie können **system-config-firewall** verwenden, um die IP-Ports zu aktivieren.

Tabelle 2.1. Aktivierte IP-Ports auf Red Hat Hochverfügbarkeits-Add-On Knoten

| IP-Port-Nummer | Protokoll | Komponente |
|----------------|-----------|--|
| 5404, 5405 | UDP | corosync/cman (Cluster-Manager) |
| 11111 | TCP | ricci (überträgt aktualisierte Cluster-Informationen) |
| 21064 | TCP | dlm (Distributed Lock Manager) |
| 16851 | TCP | modclusterd |

2.3.2. Aktivieren von IP-Ports auf Computern, die **luci** ausführen

Um Client-Computern zu erlauben, mit einem Computer zu kommunizieren, der **luci** (den **Conga**-Benutzeroberflächen-Server) ausführt, müssen Sie die IP-Ports für **luci** aktivieren. Aktivieren Sie auf jedem Computer, der **luci** ausführt, die IP-Ports gemäß [Tabelle 2.2, „Aktivierter IP-Port auf einem Computer, der **luci** ausführt“](#).



Anmerkung

Wenn ein Cluster-Knoten **luci** ausführt, sollte der Port 11111 bereits aktiviert sein.

Tabelle 2.2. Aktivierter IP-Port auf einem Computer, der **luci ausführt**

| IP-Port-Nummer | Protokoll | Komponente |
|----------------|-----------|---|
| 8084 | TCP | luci (Conga -Benutzeroberflächen-Server) |

2.4. Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten

Falls Ihr Cluster integrierte Fencing-Geräte verwendet, müssen Sie ACPI ("Advanced Configuration and Power Interface") konfigurieren, um ein sofortiges und vollständiges Fencing (Datenabgrenzung) zu gewährleisten.

 **Anmerkung**

Werfen Sie für die aktuellsten Informationen über integrierte Fencing-Geräte, die vom Red Hat Hochverfügbarkeits-Add-On unterstützt werden, einen Blick auf http://www.redhat.com/cluster_suite/hardware/.

Falls ein Cluster-Knoten zur Abgrenzung durch ein integriertes Fencing-Gerät konfiguriert ist, deaktivieren Sie ACPI Soft-Off für diesen Knoten. Das Deaktivieren des ACPI Soft-Off erlaubt es einem integrierten Fencing-Gerät, einen Knoten sofort und vollständig abzuschalten, statt diesen sauber herunterzufahren (z.B. **shutdown -h now**). Bleibt ACPI Soft-Off dagegen aktiviert, braucht ein integriertes Fencing-Gerät vier Sekunden oder länger, um einen Knoten abzuschalten (siehe nachfolgende Anmerkung). Zudem ist mit aktiviertem ACPI Soft-Off ein integriertes Fencing-Gerät unter Umständen nicht dazu in der Lage, einen Knoten abzuschalten, der während des Herunterfahrens hängenbleibt. Unter diesen Umständen würde die Abgrenzung erst verzögert erfolgen oder ganz fehlschlagen. Wenn ein Knoten mit einem integrierten Fencing-Gerät abgegrenzt wird und ACPI Soft-Off aktiviert ist, würde sich ein Cluster infolgedessen nur sehr langsam erholen oder gar administratives Eingreifen erfordern.

 **Anmerkung**

Die Zeit, die zum Abgrenzen eines Knotens benötigt wird, hängt vom verwendeten integrierten Fencing-Gerät ab. Die Leistung einiger integrierter Fencing-Geräte ist vergleichbar mit dem gedrückt Halten des An-/Ausschaltknopfes; das Fencing-Gerät benötigt demnach etwa vier bis fünf Sekunden zum Abschalten des Knotens. Die Leistung anderer integrierter Fencing-Geräte ist vergleichbar mit einem kurzen Drücken des An-/Ausschaltknopfes; das Fencing-Gerät verlässt sich also auf das Betriebssystem zum Abschalten des Knotens und benötigt demnach eine sehr viel längere Zeit als vier oder fünf Sekunden zum Abschalten des Knotens.

Um ACPI Soft-Off zu deaktivieren, verwenden Sie den **chkconfig**-Befehl und überprüfen Sie, dass der Knoten bei einer Abgrenzung tatsächlich sofort abgeschaltet wird. Die bevorzugte Methode zum Deaktivieren von ACPI Soft-Off ist der **chkconfig**-Befehl. Falls diese Methode in Ihrem Cluster nicht das gewünschte Ergebnis erzielt, können Sie ACPI Soft-Off auch mit einer der folgenden, alternativen Methoden deaktivieren:

- ▶ Ändern Sie die BIOS-Einstellung auf "instant-off" oder auf eine ähnliche Einstellung, die den Knoten ohne Verzögerung abschaltet.

 **Anmerkung**

Das Deaktivieren von ACPI Soft-Off im BIOS steht auf einigen Computern ggf. nicht zur Verfügung.

- ▶ Fügen Sie **acpi=off** zu der Kernel-Boot-Befehlszeile der **/boot/grub/grub.conf**-Datei hinzu.

 **Wichtig**

Diese Methode deaktiviert ACPI vollständig; einige Computers fahren jedoch ggf. nicht einwandfrei hoch, wenn ACPI vollständig deaktiviert ist. Nutzen Sie diese Methode *nur dann*, wenn die anderen gezeigten Methoden für Ihren Cluster nicht zum gewünschten Ergebnis führen.

Die folgenden Abschnitte zeigen die Verfahren der bevorzugten Methode sowie der alternativen Methoden zum Deaktivieren von ACPI Soft-Off:

- ▶ [Abschnitt 2.4.1, „Deaktivieren von ACPI Soft-Off mit dem chkconfig-Befehl“](#) — Bevorzugte Methode

- ▶ [Abschnitt 2.4.2, „Deaktivieren von ACPI Soft-Off im BIOS“](#) — Erste alternative Methode
- ▶ [Abschnitt 2.4.3, „Vollständiges Deaktivieren von ACPI in der `grub.conf`-Datei“](#) — Zweite alternative Methode

2.4.1. Deaktivieren von ACPI Soft-Off mit dem `chkconfig`-Befehl

Sie können den `chkconfig`-Befehl zur Deaktivierung von ACPI Soft-Off verwenden, indem Sie entweder den ACPI-Daemon (`acpid`) aus der `chkconfig`-Verwaltung entfernen, oder indem Sie `acpid` abschalten.



Anmerkung

Dies ist die bevorzugte Methode zur Deaktivierung von ACPI Soft-Off.

Deaktivieren Sie ACPI Soft-Off auf jedem Cluster-Knoten mit dem `chkconfig`-Befehl, und zwar wie folgt:

1. Führen Sie einen dieser beiden Befehle aus:
 - ▶ `chkconfig --del acpid` — Dieser Befehl entfernt `acpid` aus der `chkconfig`-Verwaltung.
 - ODER —
 - ▶ `chkconfig --level 2345 acpid off` — Dieser Befehl schaltet `acpid` ab.
2. Starten Sie den Knoten neu.
3. Wenn der Cluster konfiguriert ist und läuft, vergewissern Sie sich, dass der Knoten bei einer Abgrenzung sofort abgeschaltet wird.



Anmerkung

Sie können den Knoten mittels `fence_node`-Befehl oder `Conga` abgrenzen.

2.4.2. Deaktivieren von ACPI Soft-Off im BIOS

Die bevorzugte Methode zum Deaktivieren von ACPI Soft-Off ist mittels `chkconfig`-Befehl ([Abschnitt 2.4.1, „Deaktivieren von ACPI Soft-Off mit dem `chkconfig`-Befehl“](#)). Führt die bevorzugte Methode jedoch nicht zum gewünschten Ergebnis, folgen Sie den in diesem Abschnitt beschriebenen Verfahren.



Anmerkung

Das Deaktivieren von ACPI Soft-Off im BIOS steht auf einigen Computern ggf. nicht zur Verfügung.

Sie können ACPI Soft-Off deaktivieren, indem Sie das BIOS in jedem Cluster-Knoten wie folgt konfigurieren:

1. Starten Sie den Knoten neu und starten Sie das **BIOS CMOS Setup Utility** Programm.
2. Navigieren Sie zum **Power**-Menü (oder ähnliches Menü zur Energieverwaltung).
3. Setzen Sie im **Power**-Menü die **Soft-Off by PWR-BTTN**-Funktion (oder ähnlich) auf **Instant-Off** (oder eine ähnliche Einstellung, die den Knoten über den An-/Ausschaltknopf ohne Verzögerung ausschaltet). [Beispiel 2.1, „BIOS CMOS Setup Utility: Soft-Off by PWR-BTTN auf Instant-Off eingestellt“](#) zeigt ein **Power**-Menü mit der **ACPI Function** auf **Enabled** (aktiviert) und **Soft-Off by PWR-BTTN** auf **Instant-Off** (sofort ausschalten) eingestellt.



Anmerkung

Abhängig von Ihrem Computertyp heißen die Menüpunkte **ACPI Function**, **Soft-Off by PWR-BTTN** und **Instant-Off** ggf. anders. Das Ziel dieses Verfahren ist es jedoch, das BIOS dahingehend zu konfigurieren, dass der Computer durch Betätigen des An-/Ausschaltknopfes ohne Verzögerung abgeschaltet wird.

4. Verlassen Sie das **BIOS CMOS Setup Utility** Programm und speichern so die BIOS-Konfiguration.
5. Wenn der Cluster konfiguriert ist und läuft, vergewissern Sie sich, dass der Knoten bei einer Abgrenzung sofort abgeschaltet wird.



Anmerkung

Sie können den Knoten mittels **fence_node**-Befehl oder **Conga** abgrenzen.

Beispiel 2.1. BIOS CMOS Setup Utility: Soft-Off by PWR-BTTN auf Instant-Off eingestellt

```

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

Dieses Beispiel zeigt die **ACPI Function** auf **Enabled** (aktiviert) und **Soft-Off by PWR-BTTN** auf **Instant-Off** (sofort ausschalten) eingestellt.

2.4.3. Vollständiges Deaktivieren von ACPI in der grub.conf-Datei

Die bevorzugte Methode zum Deaktivieren von ACPI Soft-Off ist mittels **chkconfig**-Befehl ([Abschnitt 2.4.1, „Deaktivieren von ACPI Soft-Off mit dem chkconfig-Befehl“](#)). Führt die bevorzugte Methode jedoch nicht zum gewünschten Ergebnis, können Sie ACPI Soft-Off in der Energieverwaltung des BIOS deaktivieren ([Abschnitt 2.4.2, „Deaktivieren von ACPI Soft-Off im BIOS“](#)). Falls in Ihrem Cluster keine dieser beiden Methoden zum Ziel führt, können Sie ACPI vollständig deaktivieren, indem Sie **acpi=off** an die Kernel-Boot-Befehlszeile der **grub.conf**-Datei anhängen.



Wichtig

Diese Methode deaktiviert ACPI vollständig; einige Computers fahren jedoch ggf. nicht einwandfrei hoch, wenn ACPI vollständig deaktiviert ist. Nutzen Sie diese Methode *nur dann*, wenn die anderen gezeigten Methoden für Ihren Cluster nicht zum gewünschten Ergebnis führen.

Sie können ACPI vollständig deaktivieren, indem Sie die `grub.conf`-Datei in jedem Cluster-Knoten wie folgt bearbeiten:

1. Öffnen Sie `/boot/grub/grub.conf` mit einem Texteditor.
2. Fügen Sie `acpi=off` am Ende der Kernel-Boot-Befehlszeile in `/boot/grub/grub.conf` hinzu (siehe [Beispiel 2.2, „Kernel-Boot-Befehlszeile mit angefügtem `acpi=off`“](#)).
3. Starten Sie den Knoten neu.
4. Wenn der Cluster konfiguriert ist und läuft, vergewissern Sie sich, dass der Knoten bei einer Abgrenzung sofort abgeschaltet wird.



Anmerkung

Sie können den Knoten mittels `fence_node`-Befehl oder `Conga` abgrenzen.

Beispiel 2.2. Kernel-Boot-Befehlszeile mit angefügtem `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/VolGroup00/LogVol100
#          initrd /initrd-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 (2.6.18-36.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-36.el5 ro root=/dev/VolGroup00/LogVol100
console=ttyS0,115200n8 acpi=off
        initrd /initrd-2.6.18-36.el5.img
```

In diesem Beispiel wurde `acpi=off` am Ende der Kernel-Boot-Befehlszeile — die Zeile, die mit "kernel /vmlinuz-2.6.18-36.el5" beginnt — angefügt.

2.5. Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten

Sie können Ihren Cluster auf Ihre Anforderungen zur Hochverfügbarkeit anpassen, indem Sie Hochverfügbarkeitsdienste konfigurieren. Die Schlüsselkomponente zur Verwaltung von Hochverfügbarkeitsdiensten im Red Hat Hochverfügbarkeits-Add-On, `rgmanager`, implementiert Ausfallsicherung für Standardapplikationen. Im Red Hat Hochverfügbarkeits-Add-On wird eine Applikation mit anderen Cluster-Ressourcen konfiguriert, um einen Hochverfügbarkeitsdienst zu bilden, der zur Ausfallsicherung von einem Cluster-Knoten auf einen anderen wechseln kann, ohne signifikante Unterbrechung für Cluster-Clients. Das Wechseln eines Hochverfügbarkeitsdienstes auf einen anderen

Knoten kann z.B. erfolgen, wenn ein Cluster-Knoten ausfällt oder ein Cluster-Systemadministrator den Dienst von einem Cluster-Knoten auf einen anderen verlegt (z.B. für eine geplante Betriebsunterbrechung eines Cluster-Knotens).

Um einen Hochverfügbarkeitsdienst zu erstellen, müssen Sie diesen in der Cluster-Konfigurationsdatei konfigurieren. Ein Hochverfügbarkeitsdienst besteht aus Cluster-*Ressourcen*. Cluster-Ressourcen bilden Blöcke, die Sie in der Cluster-Konfigurationsdatei erstellen und verwalten können — beispielsweise eine IP-Adresse, ein Skript zur Initialisierung einer Applikation oder eine via Red Hat GFS2 gemeinsam genutzte Partition.

Ein Hochverfügbarkeitsdienst darf zur Gewährleistung der Datenintegrität zu jeder Zeit nur auf einem einzigen Cluster-Knoten laufen. Sie können eine Ausfallsicherungspriorität in einer Ausfallsicherungs-Domain angeben. Die Angabe einer solchen Ausfallsicherungspriorität besteht aus der Zuweisung eines Prioritätslevels für jeden Knoten in einer Ausfallsicherungs-Domain. Das Prioritätslevel bestimmt die Reihenfolge der Ausfallsicherung — dabei wird ermittelt, auf welchen Knoten ein Hochverfügbarkeitsdienst im Falle eines Ausfalls wechseln soll. Falls Sie keine Ausfallsicherungspriorität angeben, kann ein Hochverfügbarkeitsdienst im Falle eines Ausfalls auf jeden beliebigen Knoten innerhalb seiner Ausfallsicherungs-Domain wechseln. Auch können Sie angeben, ob ein Hochverfügbarkeitsdienst so eingeschränkt werden soll, dass er nur auf Knoten seiner zugewiesenen Ausfallsicherungs-Domains läuft. (Ist ein Hochverfügbarkeitsdienst mit einer uneingeschränkten Ausfallsicherungs-Domain verknüpft, kann er für den Fall, dass kein Mitglied der Ausfallsicherungs-Domain zur Verfügung steht, auf jedem beliebigen Cluster-Knoten starten.)

[Abbildung 2.1. „Web-Server Cluster-Dienst Beispiel“](#) zeigt ein Beispiel eines Hochverfügbarkeitsdienstes, nämlich einen Web-Server mit der Bezeichnung "content-webserver". Er läuft auf Cluster-Knoten B und befindet sich in einer Ausfallsicherungs-Domain, die aus den Knoten A, B und D besteht. Zusätzlich ist die Ausfallsicherungs-Domain mit einer Ausfallsicherungspriorität konfiguriert, um im Falle eines Ausfalls auf den Knoten D zu wechseln, bevor auf Knoten A gewechselt wird und um die Ausfallsicherung nur auf Knoten aus dieser Ausfallsicherungs-Domain zu beschränken. Der Hochverfügbarkeitsdienst umfasst die folgenden Cluster-Ressourcen:

- ▶ IP-Adressen-Ressource — IP-Adresse 10.10.10.201.
- ▶ Eine Applikations-Ressource mit dem Namen "httpd-content" — Ein Init-Skript `/etc/init.d/httpd` für eine Web-Server-Applikation (legt **httpd** fest).
- ▶ Eine Dateisystem-Ressource — Red Hat GFS2, genannt "gfs2-content-webserver".

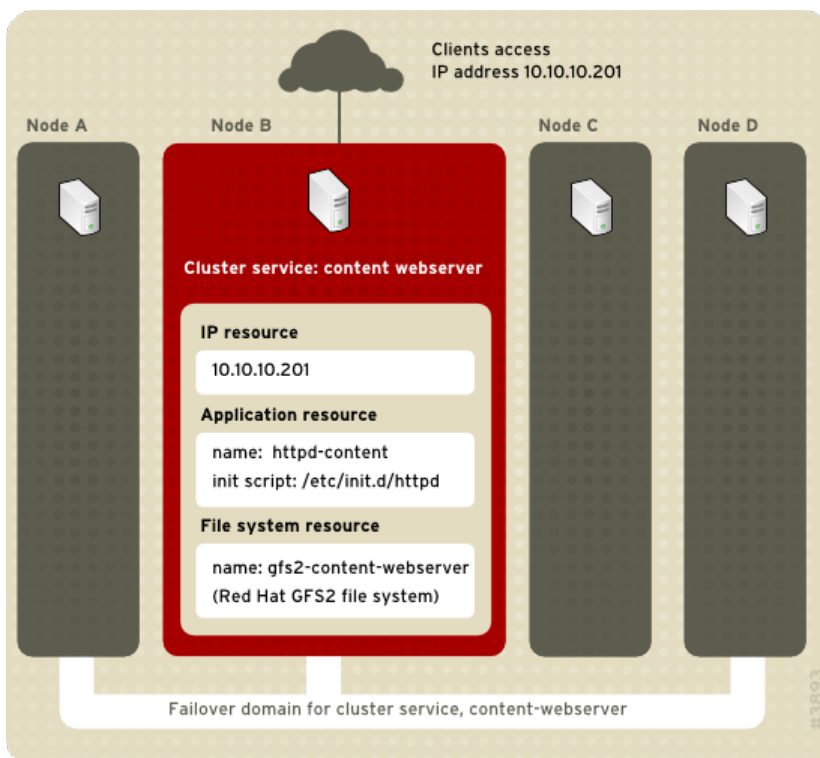


Abbildung 2.1. Web-Server Cluster-Dienst Beispiel

Clients greifen auf den Cluster-Dienst via IP-Adresse 10.10.10.201 zu, was eine Interaktion mit der Web-Server-Applikation, `httpd-content`, ermöglicht. Die Applikation "`httpd-content`" verwendet das "`gfs2-content-webserver`"-Dateisystem. Falls der Knoten B ausfallen sollte, würde der Hochverfügbarkeitsdienst "`content-webserver`" auf Knoten D wechseln. Falls Knoten D nicht verfügbar sein sollte, oder auch ausgefallen ist, würde der Dienst auf Knoten A wechseln. Die Ausfallsicherung würde ohne nennenswerte Unterbrechung für Cluster-Clients erfolgen. In einem HTTP-Dienst beispielsweise könnten hierdurch lediglich gewisse Zustandsinformationen verloren gehen (z.B. Sitzungsdaten). Der Hochverfügbarkeitsdienst wäre von einem anderen Cluster-Knoten aus unter derselben IP-Adresse erreichbar, wie vor der Ausfallsicherung.



Anmerkung

Weitere Informationen über Hochverfügbarkeitsdienste und Ausfallsicherungs-Domains finden Sie im Handbuch *Überblick über das Hochverfügbarkeits-Add-On*. Informationen über die Konfiguration von Ausfallsicherungs-Domains finden Sie in [Kapitel 3, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#) (unter Verwendung von **Conga**) oder [Kapitel 7, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#) (unter Verwendung der Befehlszeilen-Tools).

Ein Hochverfügbarkeitsdienst besteht aus einer Gruppe von Cluster-Ressourcen, die als eine zusammenhängende Einheit konfiguriert wurden und zusammen einen spezialisierten Dienst für Clients bereitstellen. Ein Hochverfügbarkeitsdienst wird als Ressourcenbaum in der Cluster-Konfigurationsdatei `/etc/cluster/cluster.conf` dargestellt (in jedem Cluster-Knoten). In der Cluster-Konfigurationsdatei ist jeder Ressourcenbaum eine XML-Darstellung, die jede Ressource spezifiziert, deren Parameter, sowie ihre Relationen zu anderen Ressourcen im Ressourcenbaum (Eltern-, Kind-, Geschwisterrelationen).



Anmerkung

Da ein Hochverfügbarkeitsdienst aus Ressourcen besteht, die in einem hierarchischen Baum angeordnet sind, wird ein solcher Dienst manchmal auch als *Ressourcenbaum* oder *Ressourcengruppe* bezeichnet. Beide Ausdrücke sind Synonyme für *Hochverfügbarkeitsdienst*.

An der Wurzel (Root) eines jeden Ressourcenbaums befindet sich eine besondere Art von Ressource — eine *Dienstressource*. Andere Arten von Ressourcen bilden den Rest eines Dienstes und bestimmen so dessen Charakteristiken. Zum Erstellen eines Hochverfügbarkeitsdienstes gehört das Erstellen einer Dienstressource, das Erstellen untergeordneter Cluster-Ressourcen, sowie deren Anordnung in eine zusammenhängende Einheit gemäß den hierarchischen Einschränkungen des Dienstes.

Das Hochverfügbarkeits-Add-On unterstützt die folgenden Hochverfügbarkeitsdienste:

- ▶ Apache
- ▶ Applikation (Skript)
- ▶ LVM (Hochverfügbarkeits-LVM)
- ▶ MySQL
- ▶ NFS
- ▶ Open LDAP
- ▶ Oracle
- ▶ PostgreSQL 8
- ▶ Samba
- ▶ SAP
- ▶ Tomcat 6

Zwei grundlegende Überlegungen sollten bei der Konfiguration eines Hochverfügbarkeitsdienstes

berücksichtigt werden:

- ▶ Die Ressourcenarten, die zum Erstellen eines Dienstes nötig sind
- ▶ Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen

Die Arten der Ressourcen und deren Hierarchie hängen von der Art des Dienstes ab, den Sie konfigurieren.

Die Arten von Cluster-Ressourcen sind in [Anhang B, Parameter der Hochverfügbarkeitsressourcen](#) aufgelistet. Informationen über Eltern-, Kind- und Geschwisterrelationen unter den Ressourcen finden Sie in [Anhang C, Verhalten der Hochverfügbarkeitsressourcen](#).

2.6. Überprüfung der Konfiguration

Die Cluster-Konfiguration wird während des Starts und beim Neuladen einer Konfiguration automatisch anhand des Cluster-Schemas unter `/usr/share/cluster/cluster.rng` überprüft. Zudem können Sie jederzeit eine Cluster-Konfiguration mithilfe des `ccs_config_validate`-Befehls überprüfen.

Ein annotiertes Schema steht unter `/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html` zur Ansicht (z.B. `/usr/share/doc/cman-3.0.12/cluster_conf.html`).

Bei der Konfigurationsprüfung wird auf folgende Fehler hin überprüft:

- ▶ XML-Gültigkeit — Überprüft, ob die Konfigurationsdatei eine gültige XML-Datei ist.
- ▶ Konfigurationsoptionen — Überprüft, ob Optionen (XML-Elemente und Parameter) gültig sind.
- ▶ Optionswerte — Überprüft, ob die Optionen gültige Daten enthalten (begrenzt).

Die folgenden Beispiele zeigen eine gültige Konfiguration und mehrere ungültige Konfigurationen, um die Gültigkeitsüberprüfungen zu veranschaulichen:

- ▶ Gültige Konfiguration — [Beispiel 2.3, „cluster.conf Beispielkonfiguration: Gültige Datei“](#)
- ▶ Ungültiges XML — [Beispiel 2.4, „cluster.conf Beispielkonfiguration: Ungültiges XML“](#)
- ▶ Ungültige Option — [Beispiel 2.5, „cluster.conf Beispielkonfiguration: Ungültige Option“](#)
- ▶ Ungültiger Optionswert — [Beispiel 2.6, „cluster.conf Beispielkonfiguration: Ungültiger Optionswert“](#)

Beispiel 2.3. ccluster.conf Beispielkonfiguration: Gültige Datei

```
<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>
```

Beispiel 2.4. ccluster.conf Beispielkonfiguration: Ungültiges XML

```
<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 diesem Beispiel fehlt in der letzten Zeile der Konfiguration (hier annotiert als "INVALID", also ungültig) ein Schrägstrich — es steht hier **<cluster>** anstelle von **</cluster>**.

Beispiel 2.5. ccluster.conf Beispielkonfiguration: Ungültige Option

```
<cluster name="mycluster" config_version="1">
  <logging 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 diesem Beispiel enthält die zweite Zeile der Konfiguration (hier annotiert als "INVALID", also ungültig) ein ungültiges XML-Element — es steht hier **logging** anstelle von **logging**.

Beispiel 2.6. ccluster.conf Beispielkonfiguration: Ungültiger Optionswert

```
<cluster name="mycluster" config_version="1">
  <logging 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 diesem Beispiel enthält die vierte Zeile der Konfiguration (hier annotiert als "INVALID", also ungültig) einen ungültigen Wert für das XML-Attribut, **nodeid** in der **clusternode**-Zeile für **node-01.example.com**. Der Wert hier ist ein negativer Wert ("-1") anstelle eines positiven Werts ("1"). Für den **nodeid**-Parameter muss der Wert jedoch positiv sein.

2.7. Überlegungen zum NetworkManager

Die Verwendung des **NetworkManager** wird auf Cluster-Knoten nicht unterstützt. Wenn Sie den **NetworkManager** auf Ihren Cluster-Knoten installiert haben, sollten Sie diesen entweder entfernen oder deaktivieren.



Anmerkung

Der **cman**-Dienst wird nicht starten, wenn der **NetworkManager** läuft oder mithilfe des **chkconfig**-Befehls zur Ausführung konfiguriert wurde.

2.8. Überlegungen zur Verwendung von Quorum Disk

Quorum Disk ist ein plattenbasierter Quorum-Daemon, **qdiskd**, der ergänzende Heuristiken zum Bestimmen der Knotengesundheit liefert. Mit Heuristiken können Sie Faktoren bestimmen, die wichtig für die Funktion des Knotens im Falle einer Spaltung des Netzwerks sind. In einem Cluster mit vier Knoten und einer 3:1 Spaltung beispielsweise, "gewinnen" die drei Knoten für gewöhnlich automatisch aufgrund Ihrer 3-zu-1 Mehrheit. In dieser Situation wird der einzelne Knoten abgegrenzt. Mithilfe von **qdiskd** können Sie dagegen Heuristiken einrichten, die es dem einzelnen Knoten ermöglichen zu gewinnen, basierend auf dessen Zugriff auf eine kritische Ressource (z.B. ein kritischer Netzwerkpfad). Falls Ihr Cluster zusätzliche Methoden zur Bestimmung der Knotengesundheit erfordert, sollten Sie zu diesem Zweck **qdiskd** konfigurieren.



Anmerkung

Das Konfigurieren von **qdiskd** ist nur dann notwendig, wenn Sie besondere Anforderungen an die Knotengesundheit haben. Beispiel für eine besondere Anforderung wäre eine "all-but-one" (alle-außer-einem) Konfiguration. In einer "all-but-one"-Konfiguration wird **qdiskd** so konfiguriert, dass genügend Quorum-Stimmen geliefert werden, um das Quorum zu erhalten, selbst wenn nur ein einziger Knoten läuft.



Wichtig

Heuristiken und andere **qdiskd**-Parameter für Ihr Deployment hängen im Wesentlichen von den Anforderungen Ihrer Umgebung und sonstigen besonderen Anforderungen ab. Werfen Sie zum besseren Verständnis der Verwendung von Heuristiken und anderen **qdiskd**-Parametern einen Blick auf die **qdisk(5)**-Handbuchseite. Falls Sie beim Einsatz von **qdiskd** in Ihrer Umgebung Hilfe benötigen, setzen Sie sich bitte mit einem autorisierten Red Hat Support-Vertreter in Verbindung.

Wenn Sie **qdiskd** einsetzen müssen, sollten Sie folgende Überlegungen berücksichtigen:

Cluster-Knotenstimmen

Wird Quorum Disk verwendet, muss jeder Cluster-Knoten eine Stimme haben.

Zeitüberschreitung für CMAN-Mitgliedschaft

Der Timeout-Wert der CMAN-Mitgliedschaft (die Zeit, die ein Knoten nicht reagiert, bevor CMAN - kurz für Cluster-Manager - diesen Knoten als tot betrachtet, nicht mehr als Mitglied) sollte mindestens doppelt so lang sein, wie der Timeout-Wert der **qdiskd**-Mitgliedschaft. Der Grund hierfür ist der, dass der Quorum-Daemon selbst ausgefallene Knoten entdecken muss und

hierzu ggf. deutlich länger braucht als der CMAN. Der Standardwert für den CMAN-Mitgliedsschafts-Timeout beträgt 10 Sekunden. Andere umgebungsspezifische Bedingungen können das Verhältnis zwischen den Mitgliedsschafts-Timeout-Werten von CMAN und **qdiskd** beeinflussen. Falls Sie beim Anpassen des Werts für den CMAN-Mitgliedsschafts-Timeout Hilfe benötigen, setzen Sie sich bitte mit einem autorisierten Red Hat Support-Vertreter in Verbindung.

Fencing (Datenabgrenzung)

Um beim Einsatz von **qdiskd** zuverlässiges Fencing zu gewährleisten, verwenden Sie Power-Fencing. Für Cluster ohne **qdiskd** können zwar auch andere Arten von Fencing zuverlässig arbeiten, diese sind jedoch für einen Cluster, der mit **qdiskd** konfiguriert ist, nicht ausreichend zuverlässig.

Höchstanzahl von Knoten

Ein Cluster, der mit **qdiskd** konfiguriert ist, unterstützt maximal 16 Knoten. Der Grund für diese Grenze liegt in der Skalierbarkeit; eine Erhöhung der Knotenanzahl geht mit einer Erhöhung der synchronen I/O-Auslastung auf dem gemeinsam verwendeten Quorum-Plattengerät einher.

Quorum-Plattengerät

Ein Quorum-Plattengerät sollte ein gemeinsam verwendetes Blockgerät sein mit parallelem Lese-/Schreibzugriff für alle Knoten in einem Cluster. Die Mindestgröße für das Blockgerät sollte 10 Megabytes betragen. Zu den gemeinsam verwendeten Blockgeräten, die von **qdiskd** verwendet werden können, gehören z.B. Multi-Port SCSI RAID Arrays, Fibre Channel RAID SAN oder RAID-konfigurierte iSCSI-Ziele. Sie können eine Quorum-Platte mithilfe von **mkqdisk** erstellen, dem Dienstprogramm für Cluster-Quorum-Platten. Weitere Informationen über die Verwendung dieses Dienstprogramms finden Sie auf dessen **mkqdisk(8)**-Handbuchseite.



Anmerkung

Der Einsatz von JBOD als Quorum-Platte wird nicht empfohlen. Eine JBOD bietet keine zuverlässige Leistung und könnte daher einem Knoten einen Schreibvorgang nicht schnell genug ermöglichen. Kann ein Knoten nicht schnell genug auf ein Quorum-Plattengerät schreiben, wird dieser Knoten fälschlicherweise aus dem Cluster ausgeschlossen.

2.9. Red Hat Hochverfügbarkeits-Add-On und SELinux

Das Hochverfügbarkeits-Add-On für Red Hat Enterprise Linux 6 unterstützt SELinux im **enforcing**-Modus mit der SELinux-Richtlinie auf **targeted** eingestellt.

Weitere Informationen über SELinux finden Sie im *Deployment-Handbuch* für Red Hat Enterprise Linux 6.

2.10. Multicast-Adressen

Red Hat Hochverfügbarkeits-Add-On-Knoten kommunizieren miteinander über Multicast-Adressen. Aus diesem Grund müssen alle Netzwerk-Switches und zugehörige Netzwerkgeräte im Red Hat Hochverfügbarkeits-Add-On so konfiguriert sein, dass Multicast-Adressen aktiviert sind und IGMP (Internet Group Management Protocol) unterstützt wird. Vergewissern Sie sich, dass sämtliche Netzwerk-Switches und zugehörige Netzwerkgeräte im Red Hat Hochverfügbarkeits-Add-On dazu in der Lage sind, Multicast-Adressen und IGMP zu unterstützen; ist dies der Fall, stellen Sie sicher, dass Multicast-Adressierung und IGMP aktiviert sind. Ohne Multicast und IGMP können nicht alle Knoten am

Cluster teilnehmen, wodurch der Cluster fehlschlagen wird.



Anmerkung

Verfahren zur Konfiguration von Netzwerk-Switches und zugehörigen Netzwerkgeräten unterscheiden sich je nach Produkt. Lesen Sie bitte die entsprechende Herstellerdokumentation oder andere Informationsquellen für Informationen darüber, wie für diese Netzwerk-Switches und zugehörige Netzwerkgeräte Multicast-Adressen und IGMP aktiviert werden können.

2.11. Überlegungen zu **ricci**

In Red Hat Enterprise Linux 6 löst **ricci** nunmehr **ccsd** ab. Es ist deshalb notwendig, dass **ricci** auf jedem Cluster-Knoten ausgeführt wird, um entweder mithilfe des **cman_tool -r**-Befehls, des **ccs**-Befehls oder mithilfe des **luce**-Benutzeroberflächen-Servers aktualisierte Cluster-Konfigurationsinformationen im Cluster verbreiten zu können. Sie können **ricci** starten, indem Sie **service ricci start** ausführen oder indem Sie mithilfe von **chkconfig** festlegen, dass es beim Systemstart automatisch starten soll. Informationen über das Aktivieren von IP-Ports für **ricci** finden Sie in [Abschnitt 2.3.1, „Aktivieren von IP-Ports auf Cluster-Knoten“](#).

Ab der Red Hat Enterprise Linux 6.1 Release erfordert **ricci** ein Passwort, wenn Sie zum ersten Mal aktualisierte Cluster-Konfigurationen von einem bestimmten Knoten verbreiten möchten. Sie richten das **ricci**-Passwort nach der Installation von **ricci** auf Ihrem System ein, indem Sie als Root den Befehl **passwd ricci** für den Benutzer **ricci** ausführen.

Kapitel 3. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga

Dieses Kapitel beschreibt die Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software mittels **Conga**. Informationen über die Verwendung von **Conga** zur Verwaltung eines laufenden Clusters finden Sie in [Kapitel 4, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga*](#).



Anmerkung

Conga ist eine grafische Benutzeroberfläche, mithilfe derer Sie das Red Hat Hochverfügbarkeits-Add-On verwalten können. Beachten Sie jedoch, dass Sie ein umfassend gutes Verständnis der zugrunde liegenden Konzepte haben sollten, um diese Oberfläche effektiv einsetzen zu können. Wir raten Ihnen davon ab, sich das Wissen über Cluster-Konfiguration durch simples Ausprobieren der verfügbaren Funktionen der Benutzeroberfläche anzueignen, da dies ein System zur Folge haben könnte, das nicht widerstandsfähig genug ist, um auch im Falle von ausgefallenen Komponenten alle Dienste am Laufen zu erhalten.

Dieses Kapitel umfasst die folgenden Abschnitte:

- ▶ [Abschnitt 3.1, „Konfigurationsaufgaben“](#)
- ▶ [Abschnitt 3.2, „Starten von luci“](#)
- ▶ [Abschnitt 3.3, „Erstellen eines Clusters“](#)
- ▶ [Abschnitt 3.4, „Globale Cluster-Eigenschaften“](#)
- ▶ [Abschnitt 3.5, „Konfiguration von Fencing-Geräten“](#)
- ▶ [Abschnitt 3.6, „Konfiguration des Fencing für Cluster-Mitglieder“](#)
- ▶ [Abschnitt 3.7, „Konfiguration einer Ausfallsicherungs-Domain“](#)
- ▶ [Abschnitt 3.8, „Konfiguration von globalen Cluster-Eigenschaften“](#)
- ▶ [Abschnitt 3.9, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#)

3.1. Konfigurationsaufgaben

Zur Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software mit **Conga** gehören die folgenden Schritte:

1. Konfiguration und Ausführen der **Conga**-Konfigurations-Benutzeroberfläche — der **luci**-Server. Siehe [Abschnitt 3.2, „Starten von luci“](#).
2. Erstellen eines Clusters. Siehe [Abschnitt 3.3, „Erstellen eines Clusters“](#).
3. Konfiguration von globalen Cluster-Eigenschaften. Siehe [Abschnitt 3.4, „Globale Cluster-Eigenschaften“](#).
4. Konfiguration von Fencing-Geräten. Siehe [Abschnitt 3.5, „Konfiguration von Fencing-Geräten“](#).
5. Konfiguration von Fencing für Cluster-Mitglieder. Siehe [Abschnitt 3.6, „Konfiguration des Fencing für Cluster-Mitglieder“](#).
6. Erstellen von Ausfallsicherungs-Domains. Siehe [Abschnitt 3.7, „Konfiguration einer Ausfallsicherungs-Domain“](#).
7. Erstellen von Ressourcen. Siehe [Abschnitt 3.8, „Konfiguration von globalen Cluster-Eigenschaften“](#).
8. Erstellen von Cluster-Diensten. Siehe [Abschnitt 3.9, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#).

3.2. Starten von luci

Installation von ricci

Um **luci** zur Konfiguration eines Clusters einsetzen zu können, muss **ricci** auf den Cluster-Knoten installiert sein und laufen, wie in [Abschnitt 2.11, „Überlegungen zu ricci“](#) beschrieben. Wie in diesem Abschnitt beschrieben, erfordert die Verwendung von **ricci** ein Passwort. **luci** fordert Sie bei der Erstellung eines Clusters für jeden Cluster-Knoten zur Eingabe dieses Passworts auf, wie in [Abschnitt 3.3, „Erstellen eines Clusters“](#) beschrieben. Vergewissern Sie sich vor dem Start von **luci**, dass die IP-Ports auf allen Cluster-Knoten, mit denen **luci** kommunizieren wird, Verbindungen zu Port 11111 vom **luci**-Server erlauben. Siehe [Abschnitt 2.3.1, „Aktivieren von IP-Ports auf Cluster-Knoten“](#) für Informationen über das Aktivieren von IP-Ports auf Cluster-Knoten.

Um das Red Hat Hochverfügbarkeits-Add-On mit **Conga** zu verwalten, installieren und starten Sie **luci** wie folgt:

1. Wählen Sie einen Computer, der **luci** hosten soll, und installieren Sie die **luci**-Software auf diesem Computer. Zum Beispiel:

```
# yum install luci
```

Anmerkung

In der Regel wird **luci** von einem Computer in einem Server Cage oder Rechenzentrum gehostet, doch auch ein Computer im Cluster kann **luci** hosten.

2. Starten Sie **luci** mittels `service luci start`. Zum Beispiel:

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

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

3. Geben Sie in einem Webbrowser die URL des **luci**-Servers in die Adressleiste ein und klicken auf **Go** (oder ähnlich). Die URL-Syntax für den **luci**-Server lautet **https://luci_server_hostname:8084**. Beim ersten Zugriff auf **luci** erscheint eine Eingabeaufforderung hinsichtlich des selbst signierten SSL-Zertifikats. Nach Bestätigung dieser Dialogfelder zeigt Ihr Webbrowser nun die **luci**-Anmeldeseite.
4. Geben Sie auf der **luci**-Anmeldeseite die Berechtigungsnachweise für einen beliebigen Benutzer für das System an, auf dem **luci** gehostet wird.
5. Nach erfolgreicher Anmeldung zeigt **luci** die **Homepage**-Seite, wie in [Abbildung 3.1, „luci Homepage-Seite“](#) dargestellt.

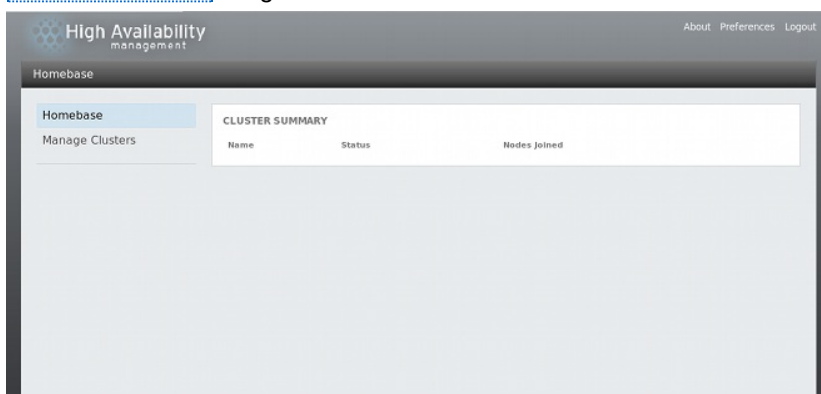


Abbildung 3.1. luci Homepage-Seite

3.3. Erstellen eines Clusters

Zum Erstellen eines Clusters mit **luci** gehört das Benennen des Clusters, das Hinzufügen von Knoten zum Cluster, Eingabe ihrer jeweiligen **ricci**-Passwörter, und Abschicken der Anfrage zur Cluster-Erstellung. Sind die Knotenangaben und -passwörter korrekt, installiert **Conga** automatisch Software auf den Cluster-Knoten (sofern die richtigen Software-Pakete nicht bereits installiert sind) und startet den Cluster. Erstellen Sie einen Cluster wie folgt:

1. Klicken Sie auf **Manage Clusters** (Cluster verwalten) im Menü auf der linken Seite der **luci Homebase**-Seite. Der **Clusters**-Bildschirm erscheint, wie in [Abbildung 3.2, „luci-Seite zur Cluster-Verwaltung“](#) dargestellt.

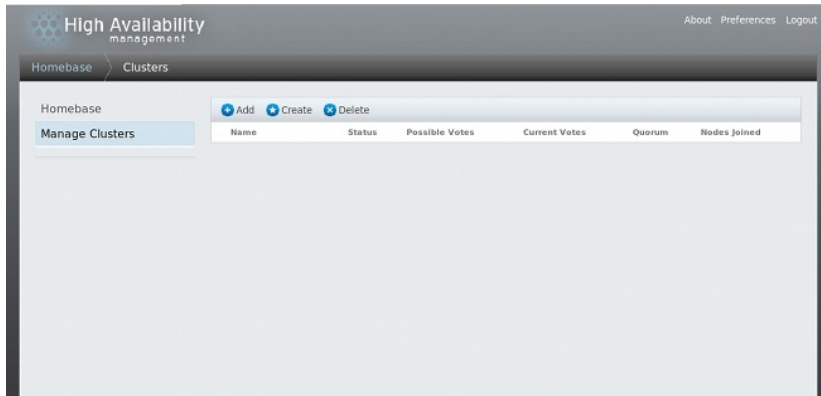


Abbildung 3.2. luci-Seite zur Cluster-Verwaltung

2. Klicken Sie auf **Create** (Erstellen). Der Bildschirm **Create New Cluster** (Neuen Cluster erstellen) erscheint, wie in [Abbildung 3.3, „luci-Dialogfeld zur Cluster-Erstellung“](#) dargestellt.

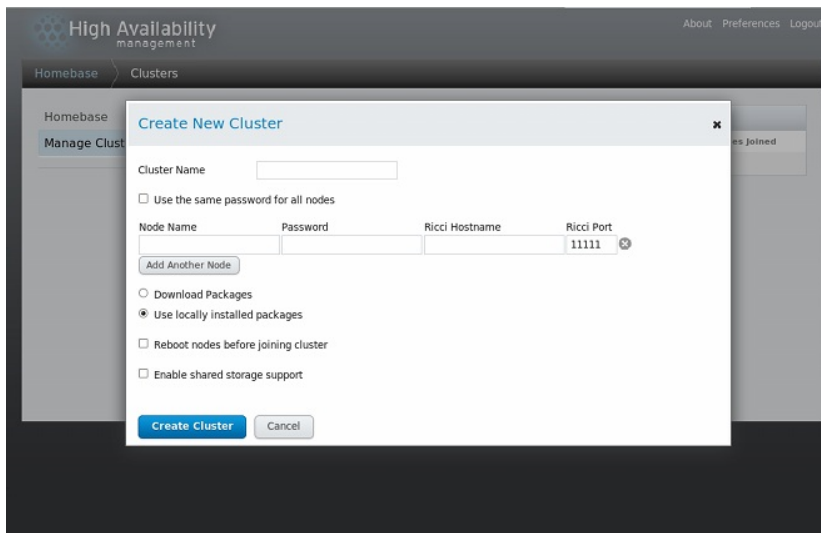


Abbildung 3.3. luci-Dialogfeld zur Cluster-Erstellung

3. Geben Sie im Dialogfeld **Create New Cluster** die folgenden Parameter ein:
 - ▶ Geben Sie im Textfeld **Cluster Name** einen Cluster-Namen ein. Der Cluster-Name darf nicht länger als 15 Zeichen sein.
 - ▶ Falls alle Knoten im Cluster dasselbe **ricci**-Passwort haben, können Sie das Auswahlkästchen **Use the same password for all nodes** (Dasselbe Passwort für alle Knoten verwenden) markieren, um beim Hinzufügen weiterer Knoten das Passwort automatisch in das entsprechende Feld einzutragen.
 - ▶ Geben Sie in der Spalte **Node Name** den Knotennamen für einen Knoten im Cluster ein und geben Sie in der Spalte **Password** das **ricci**-Passwort für den Knoten ein.
 - ▶ Falls Ihr System mit einem dedizierten privaten Netzwerk konfiguriert ist, das ausschließlich für

Cluster-Datenverkehr genutzt wird, können Sie **luci** dahingehend konfigurieren, dass die Kommunikation mit **ricci** auf einer Adresse erfolgt, die sich von der Adresse unterscheidet, in die der Cluster-Knotenname aufgelöst wird. Sie erreichen dies, indem Sie diese Adresse als **Ricci Hostname** festlegen.

- ▶ Falls Sie einen anderen Port für den **ricci**-Agent als den Standard 11111 verwenden, können Sie diesen Parameter hier ändern.
- ▶ Klicken Sie auf **Add Another Node** (Weiteren Knoten hinzufügen) und geben Sie den Knotennamen und das **ricci**-Passwort für jeden weiteren Knoten im Cluster ein.
- ▶ Falls Sie beim Erstellen des Clusters nicht die bereits auf den Knoten installierten Cluster-Software-Pakete aktualisieren möchten, lassen Sie die Option **Use locally installed packages** (Lokal installierte Pakete verwenden) ausgewählt. Falls Sie dagegen alle Cluster-Software-Pakete aktualisieren möchten, wählen Sie die Option **Download Packages** (Pakete herunterladen).



Anmerkung

Ungeachtet dessen, ob Sie die Option **Use locally installed packages** oder **Download Packages** wählen, werden eventuell fehlende Basis-Cluster-Komponenten (**cman**, **rgmanager**, **modcluster** samt Abhängigkeiten) installiert. Falls diese nicht installiert werden können, schlägt die Knotenerstellung fehl.

- ▶ Wählen Sie **Reboot nodes before joining cluster** (Knoten vor Cluster-Beitritt neu starten) falls gewünscht.
 - ▶ Wählen Sie **Enable shared storage support** (Unterstützung für gemeinsam verwendeten Speicher aktivieren), falls geclusterter Speicher erforderlich ist; dadurch werden die Pakete heruntergeladen, die Unterstützung für geclusterter Speicher hinzufügen, und geclusterter LVM wird aktiviert. Sie sollten dies nur dann auswählen, wenn Sie Zugriff auf das Resilient Storage Add-On oder das Scalable File System Add-On haben.
4. Klicken Sie auf **Create Cluster** (Cluster erstellen). Der Klick auf **Create Cluster** löst die folgenden Aktionen aus:
- a. Falls Sie **Download Packages** (Pakete herunterladen) ausgewählt haben, werden die Cluster-Software-Pakete auf die Knoten heruntergeladen.
 - b. Cluster-Software wird auf den Knoten installiert (bzw. es wird überprüft, ob die richtigen Software-Pakete installiert sind).
 - c. Die Cluster-Konfigurationsdatei wird aktualisiert und an jeden Knoten im Cluster weitergereicht.
 - d. Die hinzugefügten Knoten treten dem Cluster bei.

Eine Meldung wird angezeigt, die besagt, dass der Cluster derzeit erstellt wird. Sobald der Cluster bereit ist, wird der Status des neu erstellten Clusters angezeigt, wie in [Abbildung 3.4, „Anzeige der Cluster-Knoten“](#) dargestellt. Beachten Sie, dass die Cluster-Erstellung fehlschlagen wird, wenn **ricci** auf keinem der Knoten ausgeführt wird.

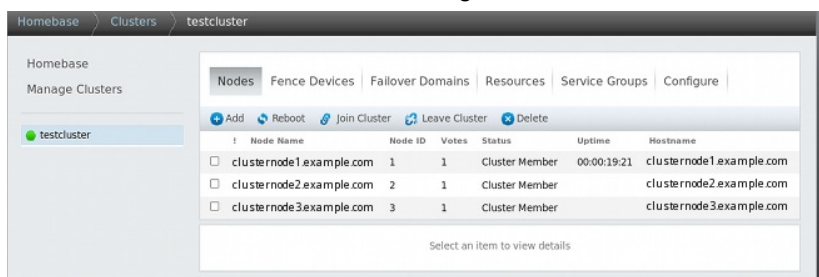


Abbildung 3.4. Anzeige der Cluster-Knoten

5. Nachdem Sie **Create Cluster** geklickt haben, um den Cluster zu erstellen, können Sie weitere Knoten zum Cluster hinzufügen oder Knoten aus ihm entfernen, indem Sie auf die **Add** (Hinzufügen) oder **Delete** (Löschen) Funktion oben auf der Cluster-Knoten-Ansichtsseite klicken. Vor dem Löschen von Knoten müssen diese gestoppt werden, es sei denn, Sie löschen den

gesamten Cluster. Weitere Informationen über das Löschen eines Knotens aus einem laufenden Cluster finden Sie in [Abschnitt 4.2.4, „Ein Mitglied aus einem Cluster löschen“](#).

3.4. Globale Cluster-Eigenschaften

Wenn Sie einen zu konfigurierenden Cluster auswählen, wird eine clusterspezifische Seite angezeigt. Diese Seite bietet eine Oberfläche zur Konfiguration von clusterweiten Eigenschaften. Sie können clusterweite Eigenschaften konfigurieren, indem Sie auf **Configure** (Konfigurieren) oben in der Cluster-Anzeige klicken. Daraufhin erscheint eine Oberfläche mit mehreren Reitern: **General** (Allgemein), **Fence Daemon** (Fencing-Daemon), **Network** (Netzwerk), **QDisk** und **Logging** (Protokollierung). Um die Parameter auf diesen Reitern zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt. Falls Sie auf einem bestimmten Reiter keine Parameter verändern möchten, überspringen Sie einfach die Schritte für den entsprechenden Reiter.

3.4.1. Konfiguration der allgemeinen Eigenschaften

Ein Klick auf den **General**-Reiter zeigt die **General Properties**-Seite (Allgemeine Eigenschaften), die eine Oberfläche bietet zur Änderung der Konfigurationsversion.

- Das Textfeld **Cluster Name** zeigt den Cluster-Namen, es akzeptiert jedoch keine Änderung des Cluster-Namens. Die einzige Möglichkeit, den Namen eines Clusters zu ändern, ist das Erstellen einer neuen Cluster-Konfiguration mit dem neuen Namen.
- Der Wert für die **Configuration Version** (Konfigurationsversion) ist standardmäßig auf **1** gesetzt und wird jedes Mal automatisch erhöht, wenn Sie Ihre Cluster-Konfiguration ändern. Falls Sie jedoch einen abweichenden Wert angeben müssen, können Sie diesen manuell im Textfeld **Configuration Version** angeben.

Falls Sie den **Configuration Version** Wert verändert haben, klicken Sie auf **Apply** (Anwenden), damit diese Änderung wirksam wird.

3.4.2. Konfiguration der Fencing-Geräteeigenschaften

Ein Klick auf den **Fence Daemon**-Reiter zeigt die **Fence Daemon Properties**-Seite (Fencing-Daemon Eigenschaften), die eine Oberfläche bietet zur Konfiguration von **Post fail delay** und **Post join delay**. Die Werte, die Sie für diese Parameter einstellen, sind allgemeine Fencing-Eigenschaften für den gesamten Cluster. Um bestimmte Fencing-Geräte für Knoten im Cluster zu konfigurieren, verwenden Sie den Menüpunkt **Fence Devices** (Fencing-Geräte) in der Cluster-Anzeige, wie in [Abschnitt 3.5, „Konfiguration von Fencing-Geräten“](#) beschrieben.

- Der Parameter **Post fail delay** (Verzögerung nach Ausfall) ist die Anzahl von Sekunden, die der Fencing-Daemon (**fenced**) wartet, bevor ein Knoten (ein Mitglied der Fencing-Domain) nach dessen Ausfall abgegrenzt wird. Der Standardwert für **Post fail delay** ist **0**. Dieser Wert kann je nach Cluster- und Netzwerkleistung angepasst werden.
- Der Parameter **Post join delay** (Verzögerung nach Beitritt) ist die Anzahl von Sekunden, die der Fencing-Daemon (**fenced**) wartet, bevor ein Knoten abgegrenzt wird, nachdem dieser der Fencing-Domain beigetreten ist. Der Standardwert für **Post join delay** ist **3**. Ein typischer Wert für **Post join delay** beträgt zwischen 20 und 30 Sekunden, kann sich jedoch je nach Cluster- und Netzwerkleistung unterscheiden.

Geben Sie die erforderlichen Werte ein und klicken auf **Apply**, damit diese Änderungen wirksam werden.



Anmerkung

Weitere Informationen über **Post join delay** und **Post fail delay** finden Sie auf der fenced(8)-Handbuchseite.

3.4.3. Netzwerkkonfiguration

Ein Klick auf den **Network**-Reiter zeigt die **Network Configuration**-Seite (Netzwerkkonfiguration), die eine Oberfläche zur Konfiguration des Netzwerktransporttyps bietet.

Sie können auf diesem Reiter eine der folgenden Optionen wählen:

- ▶ **UDP multicast and let cluster choose the multicast address** (UDP-Multicast und den Cluster die Multicast-Adresse auswählen lassen)

Dies ist die Standardeinstellung. Wenn Sie diese Option auswählen, erstellt die Red Hat Hochverfügbarkeits-Add-On-Software eine Multicast-Adresse basierend auf der Cluster-ID. Es generiert die unteren 16 Bits der Adresse und fügt diese dem oberen Teil der Adresse an, abhängig davon, ob das IP-Protokoll IPV4 oder IPV6 verwendet wird:

- Bei IPV4 — Die gebildete Adresse ist 239.192. plus die von der Red Hat Hochverfügbarkeits-Add-On-Software generierten unteren 16 Bits.
- Bei IPV6 — Die gebildete Adresse ist FF15:: plus die von der Red Hat Hochverfügbarkeits-Add-On-Software generierten unteren 16 Bits.



Anmerkung

Die Cluster-ID ist eine eindeutige Kennung, die **cman** für jeden Cluster generiert. Um die Cluster-ID einzusehen, führen Sie den Befehl **cman_tool status** auf einem Cluster-Knoten aus.

- ▶ **UDP multicast and specify the multicast address manually** (UDP-Multicast und manuell die Multicast-Adresse angeben)

Falls Sie eine bestimmte Multicast-Adresse verwenden müssen, wählen Sie diese Option und geben Sie im Textfeld eine Multicast-Adresse an.

Falls Sie eine Multicast-Adresse angeben, sollten Sie die 239.192.x.x Serie (oder FF15:: für IPv6) nutzen, die **cman** verwendet. Falls Sie eine Multicast-Adresse außerhalb dieses Bereichs verwenden, kann dies andernfalls zu unvorhergesehenem Verhalten führen. So könnte z.B. die Adresse 224.0.0.x (d.h. "Alle Hosts auf dem Netzwerk") unter Umständen von mancher Hardware nicht korrekt oder gar nicht geroutet werden.



Anmerkung

Falls Sie eine Multicast-Adresse angeben, überprüfen Sie die Konfiguration der Router, die von Cluster-Paketen durchquert werden. Manche Router brauchen eine lange Zeit zum Lernen von Adressen, was sich drastisch auf die Cluster-Leistung auswirken kann.

Klicken Sie auf **Apply** (Anwenden). Wenn Sie den Transporttyp ändern, ist ein Neustart des Clusters nötig, damit die Änderungen wirksam werden.

3.4.4. Quorum-Plattenkonfiguration

Ein Klick auf den **QDisk**-Reiter zeigt die **Quorum Disk Configuration**-Seite (Quorum-Plattenkonfiguration), die eine Oberfläche zur Konfiguration von Quorum-Plattenparametern bietet, falls Sie eine Quorum-Platte verwenden müssen.



Wichtig

Quorum-Plattenparameter und Heuristiken hängen von der jeweiligen Umgebung und ggf. besonderen Anforderungen ab. Um die Verwendung von Quorum-Plattenparametern und Heuristiken zu verstehen, werfen Sie einen Blick auf die **qdisk(5)**-Handbuchseite. Falls Sie Hilfe zum Verständnis oder zur Verwendung von Quorum-Platten benötigen, setzen Sie sich bitte mit einem autorisierten Red Hat Support-Vertreter in Verbindung.

Der **Do not use a Quorum Disk**-Parameter (Keine Quorum-Platte verwenden) ist standardmäßig aktiviert. Wenn Sie eine Quorum-Platte verwenden müssen, klicken Sie auf **Use a Quorum Disk** (Quorum-Platte verwenden), geben Sie die Quorum-Plattenparameter an, klicken Sie auf **Apply** (Anwenden) und starten Sie den Cluster neu, damit die Änderungen wirksam werden.

[Tabelle 3.1, „Quorum-Plattenparameter“](#) beschreibt die Quorum-Plattenparameter.

Tabelle 3.1. Quorum-Plattenparameter

| Parameter | Beschreibung |
|---|--|
| Specify physical device: By device label | Spezifiziert das Quorum-Platten-Label, das von dem mkqdisk -Dienstprogramm erstellt wurde. Wird dieses Feld verwendet, liest der Quorum-Daemon die /proc/partitions , sucht nach qdisk-Signaturen auf jedem gefundenen Blockgerät und vergleicht das Label mit dem angegebenen Label. Dies ist in Konfigurationen hilfreich, in denen der Name des Quorum-Geräts sich von Knoten zu Knoten unterscheidet. |
| Heuristics | <p>Path to Program — Das Programm, das dazu verwendet wird zu bestimmen, ob diese Heuristik verfügbar ist. Dies kann alles sein, was durch /bin/sh -c ausgeführt werden kann. Ein Rückgabewert von 0 bedeutet eine erfolgreiche Durchführung, alles andere bedeutet ein Scheitern. Dieses Feld ist erforderlich.</p> <p>Interval — Die Zeitabstände (in Sekunden), in denen die Heuristik abgefragt wird. Das standardmäßige Intervall für jede Heuristik ist 2 Sekunden.</p> <p>Score — Das Gewicht dieser Heuristik. Seien Sie vorsichtig beim Festlegen des Gewichts für Heuristiken. Das standardmäßige Gewicht für jede Heuristik ist 1.</p> <p>TKO — Die Anzahl von aufeinander folgenden Fehlschlägen, bevor diese Heuristik für nicht verfügbar erklärt wird.</p> |
| Minimum total score | Die Mindestpunktzahl eines Knotens, bei der dieser noch als "lebendig" betrachtet wird. Falls dieser Wert weggelassen oder auf 0 gesetzt wird, so wird die Standardfunktion floor((n+1)/2) verwendet, wobei n die Summe der Heuristik-Punktzahlen ist. Der Minimum Score Wert darf nie die Summe der Heuristik-Punktzahlen übersteigen, andernfalls wird die Quorum-Platte nicht verfügbar sein. |



Anmerkung

Durch einen Klick auf **Apply** auf dem Reiter **QDisk Configuration** werden die Änderungen in die Cluster-Konfigurationsdatei (**/etc/cluster/cluster.conf**) auf jedem Cluster-Knoten übertragen. Damit die Quorum-Platte funktioniert, müssen Sie den Cluster neu starten (siehe [Abschnitt 4.3, „Starten, Stoppen, Neustarten und Löschen von Clustern“](#)).

3.4.5. Konfiguration der Protokollierung

Ein Klick auf den **Logging**-Reiter (Protokollierung) zeigt die **Logging Configuration**-Seite (Konfiguration der Protokollierung), die eine Oberfläche zur Konfiguration der Protokollierungseinstellungen bietet.

Die folgenden Einstellungen können Sie für die globale Protokollierungskonfiguration festlegen:

- ▶ Wenn Sie **Log debugging messages** (Debugging-Nachrichten protokollieren) auswählen, werden Debugging-Nachrichten in der Protokolldatei gespeichert.
- ▶ Wenn Sie **Log messages to syslog** (Nachrichten mit syslog protokollieren) auswählen, werden

Nachrichten mit **syslog** protokolliert. Sie können die **syslog message facility** und die **syslog message priority** auswählen. Die Einstellung **syslog message priority** (Syslog Nachrichtenpriorität) legt fest, dass Nachrichten mit der ausgewählten Priorität oder höher an **syslog** gesendet werden.

- Wenn Sie **Log messages to log file** (Nachrichten in Protokolldatei speichern) auswählen, werden Nachrichten in der Protokolldatei gespeichert. Sie können den Pfadnamen der Protokolldatei angeben. Die Einstellung **logfile message priority** legt fest, dass Nachrichten mit der ausgewählten Priorität oder höher in der Protokolldatei gespeichert werden.

Sie können die globalen Protokollierungseinstellungen für bestimmte Daemons außer Kraft setzen, indem Sie einen der Daemons unten auf der **Logging Configuration**-Seite auswählen. Nachdem Sie den Daemon ausgewählt haben, können Sie auswählen, ob die Debugging-Nachrichten für diesen Daemon protokolliert werden sollen. Sie können auch **syslog** und Protokolldateieinstellungen für diesen Daemon vornehmen.

Klicken Sie auf **Apply**, damit die Änderungen an der Protokollierungskonfiguration wirksam werden.

3.5. Konfiguration von Fencing-Geräten

Die Konfiguration von Fencing-Geräten umfasst das Erstellen, Aktualisieren und Löschen von Fencing-Geräten für den Cluster. Sie müssen die Fencing-Geräte in einem Cluster konfigurieren, bevor Sie Fencing für die Knoten im Cluster konfigurieren können.

Zum Erstellen eines Fencing-Geräts gehört die Auswahl eines Fencing-Gerätetyps und die Eingabe der Parameter für das Fencing-Gerät (z.B. Name, IP-Adresse, Login und Passwort). Das Aktualisieren eines Fencing-Geräts umfasst die Auswahl eines vorhandenen Fencing-Geräts und das Ändern von Parametern für dieses Fencing-Gerät. Zum Löschen eines Fencing-Geräts gehört die Auswahl eines vorhandenen Fencing-Geräts und das Löschen desselben.

Dieser Abschnitt beschreibt die Verfahren für die folgenden Aufgaben:

- Erstellen von Fencing-Geräten — Siehe [Abschnitt 3.5.1, „Erstellen eines Fencing-Geräts“](#). Nachdem Sie ein Fencing-Gerät erstellt und benannt haben, können Sie die Fencing-Geräte für jeden Knoten im Cluster konfigurieren wie in [Abschnitt 3.6, „Konfiguration des Fencing für Cluster-Mitglieder“](#) beschrieben.
- Aktualisieren von Fencing-Geräten — Siehe [Abschnitt 3.5.2, „Ändern eines Fencing-Geräts“](#).
- Löschen von Fencing-Geräten — Siehe [Abschnitt 3.5.3, „Löschen eines Fencing-Geräts“](#).

Auf der clusterspezifischen Seite können Sie Fencing-Geräte für diesen Cluster konfigurieren, indem Sie auf **Fence Devices** (Fencing-Geräte) oben in der Cluster-Anzeige klicken. Daraufhin werden die Fencing-Geräte für den Cluster angezeigt, sowie die folgenden Menüpunkte zur Konfiguration der Fencing-Geräte: **Add** (Hinzufügen), **Update** (Aktualisieren) und **Delete** (Löschen). Dies ist der Ausgangspunkt für alle Verfahren, die in den folgenden Abschnitten beschrieben werden.



Anmerkung

Falls es sich hierbei um die anfängliche Cluster-Konfiguration handelt, wurden noch keine Fencing-Geräte erstellt, weshalb in diesem Fall keine Geräte angezeigt werden.

[Abbildung 3.5, „luci-Seite zur Konfiguration von Fencing-Geräten“](#) zeigt den Konfigurationsbildschirm, bevor jegliche Fencing-Geräte erstellt wurden.

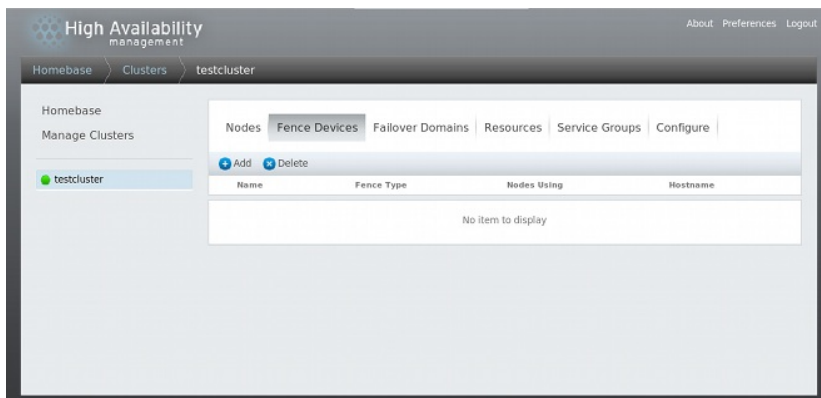


Abbildung 3.5. luci-Seite zur Konfiguration von Fencing-Geräten

3.5.1. Erstellen eines Fencing-Geräts

Um ein Fencing-Gerät zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der **Fence Devices** Konfigurationsseite auf **Add** (Hinzufügen). Durch den Klick auf **Add** wird das Dialogfenster **Add Fence Device (Instance)** (Fencing-Gerät-Instanz hinzufügen) angezeigt. Wählen Sie aus diesem Dialogfenster den zu konfigurierenden Fencing-Gerätetyp.
2. Geben Sie die nötigen Informationen im Dialogfeld **Add Fence Device (Instance)** an, je nach Typ des Fencing-Geräts. Werfen Sie einen Blick auf [Anhang A, Parameter der Fencing-Geräte](#) für weitere Informationen über Fencing-Geräteparameter. In einigen Fällen müssen Sie zusätzliche, knotenspezifische Parameter für das Fencing-Gerät angeben, wenn Sie Fencing für individuelle Knoten konfigurieren, wie in [Abschnitt 3.6, „Konfiguration des Fencing für Cluster-Mitglieder“](#) beschrieben.
3. Klicken Sie auf **Submit**.
4. Nachdem das Fencing-Gerät hinzugefügt wurde, erscheint es auf der **Fence Devices** Konfigurationsseite.

3.5.2. Ändern eines Fencing-Geräts

Um ein Fencing-Gerät zu ändern, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der **Fence Devices** Konfigurationsseite auf den Namen des zu ändernden Fencing-Geräts. Dies öffnet ein Dialogfenster für dieses Fencing-Gerät, das Ihnen die für dieses Gerät konfigurierten Werte anzeigt.
2. Um das Fencing-Gerät zu ändern, geben Sie die gewünschten Änderungen für die angezeigten Parameter ein. Siehe [Anhang A, Parameter der Fencing-Geräte](#) für weitere Informationen.
3. Klicken Sie auf **Apply** und warten Sie, bis die Konfiguration aktualisiert wurde.

3.5.3. Löschen eines Fencing-Geräts



Anmerkung

Fencing-Geräte, die derzeit in Gebrauch sind, können nicht gelöscht werden. Um ein Fencing-Gerät zu löschen, das derzeit in Gebrauch ist, aktualisieren Sie zunächst die Fencing-Konfiguration aller Knoten, die dieses Gerät verwenden, und löschen Sie anschließend das Gerät.

Um ein Fencing-Gerät zu löschen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der **Fence Devices** Konfigurationsseite das Auswahlkästchen links von dem Fencing-Gerät bzw. den Fencing-Geräten, das/die Sie löschen möchten.
2. Klicken Sie auf **Delete** und warten Sie, bis die Konfiguration aktualisiert wurde. Es wird eine

Meldung angezeigt, die bestätigt, welche Geräte gelöscht werden.

3. Sobald die Konfiguration aktualisiert wurde, erscheint das gelöschte Fencing-Gerät nicht länger in der Anzeige.

3.6. Konfiguration des Fencing für Cluster-Mitglieder

Nachdem Sie die ersten Schritte zum Erstellen eines Clusters und zum Erstellen von Fencing-Geräten abgeschlossen haben, müssen Sie nun das Fencing für die Cluster-Knoten konfigurieren. Um das Fencing für die Knoten zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt. Beachten Sie, dass Sie das Fencing für jeden Knoten im Cluster konfigurieren müssen.

Die folgenden Abschnitte beschreiben das Verfahren zur Konfiguration eines einzelnen Fencing-Geräts für einen Knoten, zur Konfiguration eines Knotens mit einem Backup-Fencing-Gerät und zur Konfiguration eines Knotens mit redundanter Stromversorgung:

- ▶ [Abschnitt 3.6.1, „Konfiguration eines einzelnen Fencing-Geräts für einen Knoten“](#)
- ▶ [Abschnitt 3.6.2, „Konfiguration eines Backup-Fencing-Geräts“](#)
- ▶ [Abschnitt 3.6.3, „Konfiguration eines Knotens mit redundanter Stromversorgung“](#)

3.6.1. Konfiguration eines einzelnen Fencing-Geräts für einen Knoten

Nutzen Sie das folgende Verfahren, um einen Knoten mit einem einzelnen Fencing-Gerät zu konfigurieren.

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** (Knoten) oben in der Cluster-Anzeige, um Fencing für die Knoten im Cluster zu konfigurieren. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homepage**-Seite auf den Cluster-Namen klicken.
2. Klicken Sie auf einen Knotennamen. Durch den Klick auf einen Link für einen Knoten erscheint eine Seite für diesen Link, auf der die Konfiguration für diesen Knoten angezeigt wird.
Die knotenspezifische Seite zeigt alle Dienste an, die gegenwärtig auf dem Knoten laufen, sowie alle Ausfallsicherungs-Domains, bei denen der Knoten Mitglied ist. Sie können eine vorhandene Ausfallsicherungs-Domain ändern, indem Sie auf deren Namen klicken. Weitere Informationen über die Konfiguration von Ausfallsicherungs-Domains finden Sie in [Abschnitt 3.7, „Konfiguration einer Ausfallsicherungs-Domain“](#).
3. Klicken Sie auf der knotenspezifischen Seite unter **Fence Devices** auf **Add Fence Method** (Fencing-Methode hinzufügen).
4. Geben Sie einen **Method Name** (Methodennamen) für die Fencing-Methode ein, die Sie für diesen Knoten konfigurieren. Dies ist ein beliebiger Name, der von dem Red Hat Hochverfügbarkeits-Add-On verwendet wird; es handelt sich hierbei nicht um den DNS-Namen für das Gerät.
5. Klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm angezeigt, der nun die Methode auflistet, die Sie eben unter **Fence Devices** hinzugefügt haben.
6. Konfigurieren Sie eine Fencing-Instanz für diese Methode, indem Sie auf die Schaltfläche **Add Fence Instance** (Fencing-Instanz hinzufügen) unter der Fencing-Methode klicken. Daraufhin wird das Drop-Down-Menü **Add Fence Device (Instance)** angezeigt, aus dem Sie ein Fencing-Gerät auswählen können, das Sie vorher wie in [Abschnitt 3.5.1, „Erstellen eines Fencing-Geräts“](#) beschrieben konfiguriert haben.
7. Wählen Sie ein Fencing-Gerät für diese Methode. Falls dieses Fencing-Gerät die Konfiguration von knotenspezifischen Parametern erfordert, werden die zu konfigurierenden Parameter angezeigt. Informationen über Fencing-Parameter finden Sie unter [Anhang A, Parameter der Fencing-Geräte](#).



Anmerkung

Für andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing) ist standardmäßig **Unfencing** in der knotenspezifischen Parameteranzeige ausgewählt. Dadurch wird sichergestellt, dass ein abgegrenzter Knoten erst wieder aktiviert wird, nachdem er neu gestartet wurde. Weitere Informationen über das Aufheben der Knotenabgrenzung finden Sie auf der **fence_node(8)** Handbuchseite.

Klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm mit der Fencing-Methode und der Fencing-Instanz angezeigt.

3.6.2. Konfiguration eines Backup-Fencing-Geräts

Sie können mehrere Fencing-Methoden für einen Knoten definieren. Falls die Abgrenzung mit der ersten Methode fehlschlägt, wird das System versuchen, den Knoten mithilfe der zweiten Methode abzugrenzen, gefolgt von jeglichen zusätzlichen konfigurierten Methoden.

Nutzen Sie das folgende Verfahren, um ein Backup-Fencing-Gerät für einen Knoten zu konfigurieren.

1. Nutzen Sie das in [Abschnitt 3.6.1, „Konfiguration eines einzelnen Fencing-Geräts für einen Knoten“](#) beschriebene Verfahren, um die primäre Fencing-Methode für einen Knoten zu konfigurieren.
2. Klicken Sie unter der von Ihnen definierten primären Methode auf **Add Fence Method**.
3. Geben Sie einen Namen für die Backup-Fencing-Methode an, die Sie für diesen Knoten konfigurieren, und klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm angezeigt, der unter der primären Fencing-Methode nun auch die eben von Ihnen hinzugefügte Methode anzeigt.
4. Konfigurieren Sie eine Fencing-Instanz für diese Methode, indem Sie auf **Add Fence Instance** (Fencing-Instanz hinzufügen) klicken. Daraufhin wird ein Drop-Down-Menü angezeigt, aus dem Sie ein Fencing-Gerät auswählen können, das Sie vorher wie in [Abschnitt 3.5.1, „Erstellen eines Fencing-Geräts“](#) beschrieben konfiguriert haben.
5. Wählen Sie ein Fencing-Gerät für diese Methode. Falls dieses Fencing-Gerät die Konfiguration von knotenspezifischen Parametern erfordert, werden die zu konfigurierenden Parameter angezeigt. Informationen über Fencing-Parameter finden Sie unter [Anhang A, Parameter der Fencing-Geräte](#).

Klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm mit der Fencing-Methode und der Fencing-Instanz angezeigt.

Bei Bedarf können Sie weitere Fencing-Methoden hinzufügen. Sie können die Reihenfolge ändern, in der die Fencing-Methoden für diesen Knoten verwendet werden, indem Sie auf **Move Up** und **Move Down** klicken.

3.6.3. Konfiguration eines Knotens mit redundanter Stromversorgung

Falls Ihr Cluster mit redundanter Stromversorgung für Ihre Knoten ausgestattet ist, vergewissern Sie sich, dass Ihr Fencing derart konfiguriert ist, dass Ihre Knoten bei der Abgrenzung vollständig abgeschaltet werden. Falls Sie jede Stromversorgung als separate Fencing-Methode konfigurieren, wird jede Stromversorgung separat abgegrenzt; die zweite Stromversorgung ermöglicht es dem System, weiterhin zu laufen, selbst wenn die erste Stromversorgung abgegrenzt ist, so dass das System selbst im Endeffekt nicht abgegrenzt wird. Um ein System mit dualer Stromversorgung zu konfigurieren, müssen Sie Ihre Fencing-Geräte so konfigurieren, dass beide Stromversorgungen abgeschaltet werden und somit auch das System vollständig abgeschaltet wird. Wenn Sie Ihr System mittels **Conga** konfigurieren, müssen Sie hierzu zwei Instanzen innerhalb einer einzelnen Fencing-Methode konfigurieren.

Um das Fencing für einen Knoten mit dualer Stromversorgung zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt.

1. Bevor Sie das Fencing für einen Knoten mit redundanter Stromversorgung konfigurieren können, müssen Sie jeden der Netzschalter als Fencing-Gerät für den Cluster konfigurieren. Informationen über die Konfiguration von Fencing-Geräten finden Sie in [Abschnitt 3.5, „Konfiguration von Fencing-Geräten“](#).
2. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** (Knoten) oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homebase**-Seite auf den Cluster-Namen klicken.
3. Klicken Sie auf einen Knotennamen. Durch den Klick auf einen Link für einen Knoten erscheint eine Seite für diesen Link, auf der die Konfiguration für diesen Knoten angezeigt wird.
4. Klicken Sie auf der knotenspezifischen Seite auf **Add Fence Method** (Fencing-Methode hinzufügen).
5. Geben Sie einen Namen für die Fencing-Methode an, die Sie für diesen Knoten konfigurieren.
6. Klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm angezeigt, der nun die Methode auflistet, die Sie eben unter **Fence Devices** hinzugefügt haben.
7. Konfigurieren Sie die erste Stromversorgung als eine Fencing-Instanz für diese Methode, indem Sie auf **Add Fence Instance** klicken. Daraufhin wird ein Drop-Down-Menü angezeigt, aus dem Sie eines der Power-Fencing-Geräte auswählen können, die Sie vorher konfiguriert haben wie in [Abschnitt 3.5.1, „Erstellen eines Fencing-Geräts“](#) beschrieben.
8. Wählen Sie eines der Power-Fencing-Geräte für diese Methode und geben die entsprechenden Parameter für dieses Gerät an.
9. Klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm mit der Fencing-Methode und der Fencing-Instanz angezeigt.
10. Klicken Sie unter derselben Fencing-Methode, für die Sie das erste Power-Fencing-Gerät konfiguriert haben, auf **Add Fence Instance**. Daraufhin wird ein Drop-Down-Menü angezeigt, aus dem Sie das zweite Power-Fencing-Gerät auswählen können, das Sie vorher wie in [Abschnitt 3.5.1, „Erstellen eines Fencing-Geräts“](#) beschrieben konfiguriert haben.
11. Wählen Sie das zweite Power-Fencing-Gerät für diese Methode und geben die entsprechenden Parameter für dieses Gerät an.
12. Klicken Sie auf **Submit**. Dadurch kehren Sie zum knotenspezifischen Bildschirm mit den Fencing-Methoden und Fencing-Instanzen zurück, der nun anzeigt, dass jedes Gerät das System in der angegebenen Reihenfolge abschaltet und in der angegebenen Reihenfolge wieder anschaltet. Dies wird in [Abbildung 3.6, „Fencing-Konfiguration für duale Stromversorgung“](#) veranschaulicht.

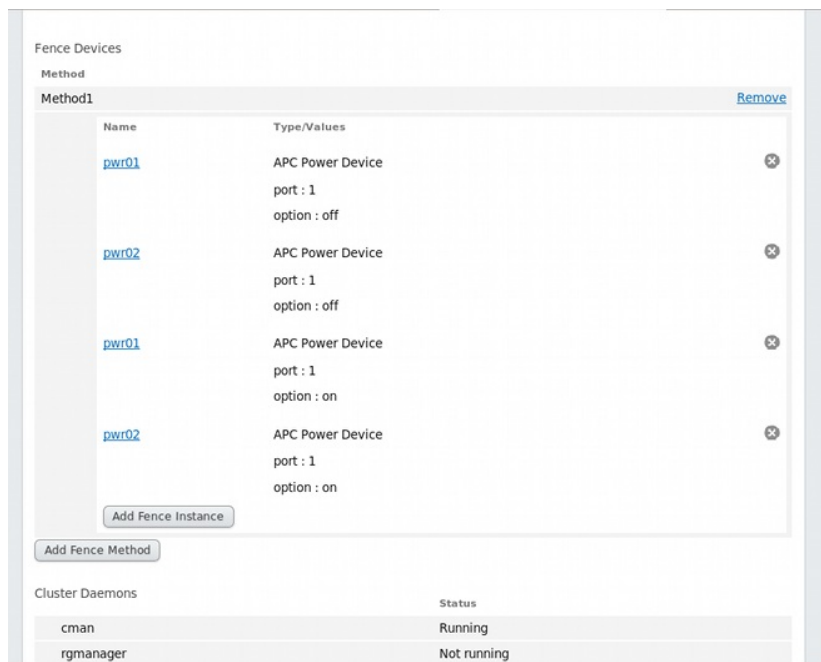


Abbildung 3.6. Fencing-Konfiguration für duale Stromversorgung

3.7. Konfiguration einer Ausfallsicherungs-Domain

Eine Ausfallsicherungs-Domain ist eine benannte Teilmenge von Cluster-Knoten, die dazu berechtigt ist, einen Cluster-Dienst im Falle eines Knotenausfalls weiterzuführen. Eine Ausfallsicherungs-Domain kann die folgenden Charakteristiken haben:

- ▶ Uneingeschränkt — Ermöglicht Ihnen, eine Teilmenge bevorzugter Mitglieder zu spezifizieren, doch der dieser Domain zugewiesene Cluster-Dienst kann auf jedem verfügbaren Mitglied ausgeführt werden.
- ▶ Eingeschränkt — Ermöglicht Ihnen, die Mitglieder einzuschränken, auf denen ein bestimmter Cluster-Dienst laufen darf. Falls keines der Mitglieder in einer eingeschränkten Ausfallsicherungs-Domain verfügbar ist, kann der Cluster-Dienst nicht gestartet werden (weder manuell noch durch die Cluster-Software).
- ▶ Ungeordnet — Wenn ein Cluster-Dienst einer ungeordneten Ausfallsicherungs-Domain zugewiesen ist, wird das Mitglied, auf dem der Cluster-Dienst ausgeführt wird, ohne Berücksichtigung von Prioritäten aus den verfügbaren Mitgliedern der Ausfallsicherungs-Domain ausgewählt.
- ▶ Geordnet — Ermöglicht Ihnen, eine Prioritätsreihenfolge für die Mitglieder einer Ausfallsicherungs-Domain anzugeben. Das erste Mitglied in der Liste wird bevorzugt, gefolgt vom zweiten Mitglied in der Liste, usw.
- ▶ Failback — Ermöglicht Ihnen festzulegen, ob ein Dienst in der Ausfallsicherungs-Domain auf den Knoten zurück wechseln soll, auf dem er vor dessen Ausfall ursprünglich ausgeführt wurde. Das Konfigurieren dieser Charakteristik ist hilfreich in Situationen, in denen ein Knoten häufig ausfällt und Teil einer geordneten Ausfallsicherungs-Domain ist. In diesem Fall würde ein Dienst, der auf dem bevorzugten Knoten in einer Ausfallsicherungs-Domain läuft, möglicherweise wiederholt zwischen dem bevorzugten Knoten und einem anderen Knoten hin- und her wechseln, was beträchtliche Leistungseinbußen zur Folge hätte.



Anmerkung

Die Failback-Charakteristik greift nur, wenn die geordnete Ausfallsicherung konfiguriert ist.



Anmerkung

Eine Änderung der Ausfallsicherungs-Domain-Konfiguration hat keine Auswirkungen auf derzeit laufende Dienste.



Anmerkung

Ausfallsicherungs-Domains werden für den Betrieb *nicht* benötigt.

Standardmäßig sind Ausfallsicherungs-Domains uneingeschränkt und ungeordnet.

In einem Cluster mit mehreren Mitgliedern kann der Einsatz einer beschränkten Ausfallsicherungs-Domain Ihnen die Arbeit erleichtern. Denn um einen Cluster zum Ausführen eines Cluster-Dienstes (wie z.B. **httpd**) einzurichten, müssen Sie auf allen Cluster-Mitgliedern, die diesen Cluster-Dienst ausführen sollen, eine identische Konfiguration einrichten. Anstatt den gesamten Cluster zur Ausführung dieses Cluster-Dienstes einzurichten, müssen Sie somit nur die Mitglieder der beschränkten Ausfallsicherungs-Domain, die Sie mit diesem Cluster-Dienst verknüpfen möchten, entsprechend einrichten.

Anmerkung

Um ein bevorzugtes Mitglied zu konfigurieren, können Sie eine uneingeschränkte Ausfallsicherungs-Domain einrichten, die nur aus einem Cluster-Mitglied besteht. Dadurch läuft der Cluster-Dienst zwar hauptsächlich auf diesem einen Cluster-Mitglied (dem bevorzugten Mitglied), doch erlaubt es dem Cluster-Dienst gleichzeitig, im Falle eines Ausfalls auf einen beliebigen anderen Knoten zu wechseln.

Die folgenden Abschnitte beschreiben das Hinzufügen, Ändern und Löschen einer Ausfallsicherungs-Domain:

- ▶ [Abschnitt 3.7.1, „Hinzufügen einer Ausfallsicherungs-Domain“](#)
- ▶ [Abschnitt 3.7.2, „Ändern einer Ausfallsicherungs-Domain“](#)
- ▶ [Abschnitt 3.7.3, „Löschen einer Ausfallsicherungs-Domain“](#)

3.7.1. Hinzufügen einer Ausfallsicherungs-Domain

Um eine Ausfallsicherungs-Domain hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Sie können auf der clusterspezifischen Seite Ausfallsicherungs-Domains für diesen Cluster konfigurieren, indem Sie auf **Failover Domains** (Ausfallsicherungs-Domains) oben in der Cluster-Ansicht klicken. Dadurch werden die Ausfallsicherungs-Domains angezeigt, die für diesen Cluster konfiguriert wurden.
2. Klicken Sie auf **Add** (Hinzufügen). Durch einen Klick auf **Add** wird das Dialogfeld **Add Failover Domain to Cluster** (Ausfallsicherungs-Domain zum Cluster hinzufügen) angezeigt, wie in [Abbildung 3.7, „luci-Dialogfeld zur Konfiguration von Ausfallsicherungs-Domains“](#) veranschaulicht.

Add Failover Domain To Cluster ✕

Name

Prioritized Order the nodes to which services failover.

Restricted Service can run only on nodes specified.

No Failback Do not send service back to 1st priority node when it becomes available again.

| | Member | Priority |
|--|--------------------------|---|
| | clusternode1.example.com | <input type="checkbox"/> <input type="text"/> |
| | clusternode2.example.com | <input type="checkbox"/> <input type="text"/> |
| | clusternode3.example.com | <input type="checkbox"/> <input type="text"/> |

Abbildung 3.7. luci-Dialogfeld zur Konfiguration von Ausfallsicherungs-Domains

3. Geben Sie im Dialogfeld **Add Failover Domain to Cluster** im Textfeld **Name** einen Namen für die Ausfallsicherungs-Domain an.

Anmerkung

Der Name sollte aussagekräftig genug sein, um daraus im Vergleich zu anderen Namen im Cluster auf den Zweck schließen zu können.

4. Um das Einstellen von Ausfallsicherungsprioritäten für Mitglieder in einer Ausfallsicherungs-Domain zu aktivieren, markieren Sie das Auswahlkästchen **Prioritized** (Priorisiert). Ist

Prioritized ausgewählt, können Sie den Prioritätswert **Priority** für jeden Knoten festlegen, der als Mitglied in der Ausfallsicherungs-Domain ausgewählt ist.

5. Um die Ausfallsicherung auf Mitglieder in dieser Ausfallsicherungs-Domain zu beschränken, markieren Sie das Auswahlkästchen **Restricted** (Eingeschränkt). Ist **Restricted** ausgewählt, werden Dienste, denen diese Ausfallsicherungs-Domain zugewiesen ist, im Fehlerfall nur auf Knoten innerhalb dieser Ausfallsicherungs-Domain wechseln.
6. Um festzulegen, dass ein Dienst in dieser Ausfallsicherungs-Domain nicht wieder auf den ursprünglichen Knoten zurück wechselt, markieren Sie das Auswahlkästchen **No Failback** (Kein Failback). Ist **No Failback** ausgewählt, so wird ein Dienst, der aufgrund eines Ausfalls von einem bevorzugten Knoten wechselt, nach dessen Wiederherstellung nicht wieder auf den ursprünglichen Knoten zurück wechseln.
7. Konfigurieren Sie Mitglieder für diese Ausfallsicherungs-Domain. Markieren Sie das Auswahlkästchen **Member** (Mitglied) für jeden Knoten, der Mitglied der Ausfallsicherungs-Domain sein soll. Falls **Prioritized** ausgewählt ist, stellen Sie im **Priority**-Textfeld die Priorität für jedes Mitglied der Ausfallsicherungs-Domain ein.
8. Klicken Sie auf **Create** (Erstellen). Dadurch wird die Seite **Failover Domains** mit der neu erstellten Ausfallsicherungs-Domain angezeigt. Eine Meldung wird angezeigt, die besagt, dass die neue Domain erstellt wird. Aktualisieren Sie die Seite, um den aktuellen Status zu sehen.

3.7.2. Ändern einer Ausfallsicherungs-Domain

Um eine Ausfallsicherungs-Domain zu ändern, folgen Sie den Schritten in diesem Abschnitt.

1. Sie können auf der clusterspezifischen Seite Ausfallsicherungs-Domains für diesen Cluster konfigurieren, indem Sie auf **Failover Domains** (Ausfallsicherungs-Domains) oben in der Cluster-Ansicht klicken. Dadurch werden die Ausfallsicherungs-Domains angezeigt, die für diesen Cluster konfiguriert wurden.
2. Klicken Sie auf den Namen einer Ausfallsicherungs-Domain. Daraufhin wird die Konfigurationsseite für diese Ausfallsicherungs-Domain angezeigt.
3. Um die **Prioritized**, **Restricted** oder **No Failback** Eigenschaften für die Ausfallsicherungs-Domain zu ändern, setzen oder entfernen Sie das Häkchen im entsprechenden Auswahlkästchen für diese Eigenschaft und klicken Sie auf **Update Properties** (Eigenschaften aktualisieren).
4. Um die Mitgliedschaften der Ausfallsicherungs-Domain zu ändern, setzen oder entfernen Sie das Häkchen im Auswahlkästchen für die gewünschten Cluster-Mitglieder. Falls die Ausfallsicherungs-Domain priorisiert ist, können Sie auch die Prioritätseigenschaft für die Cluster-Mitglieder verändern. Klicken Sie zum Abschluss auf **Update Settings** (Einstellungen aktualisieren).

3.7.3. Löschen einer Ausfallsicherungs-Domain

Um eine Ausfallsicherungs-Domain zu löschen, folgen Sie den Schritten in diesem Abschnitt.

1. Sie können auf der clusterspezifischen Seite Ausfallsicherungs-Domains für diesen Cluster konfigurieren, indem Sie auf **Failover Domains** (Ausfallsicherungs-Domains) oben in der Cluster-Ansicht klicken. Dadurch werden die Ausfallsicherungs-Domains angezeigt, die für diesen Cluster konfiguriert wurden.
2. Markieren Sie das Auswahlkästchen der zu löschenden Ausfallsicherungs-Domain.
3. Klicken Sie auf **Delete** (Löschen).

3.8. Konfiguration von globalen Cluster-Eigenschaften

Sie können globale Ressourcen konfigurieren, die von jedem Dienst im Cluster verwendet werden dürfen, und Sie können Ressourcen konfigurieren, die nur einem bestimmten Dienst zur Verfügung stehen.

Um eine globale Cluster-Ressource hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt. Sie können eine Ressource lokal für einen bestimmten Dienst hinzufügen, während Sie diesen Dienst konfigurieren, wie in [Abschnitt 3.9, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#) beschrieben.

1. Sie können auf der clusterspezifischen Seite Ressourcen für diesen Cluster hinzufügen, indem Sie auf **Resources** oben in der Cluster-Ansicht klicken. Dadurch werden die Ressourcen angezeigt, die für diesen Cluster konfiguriert wurden.
2. Klicken Sie auf **Add**. Dadurch erscheint das Drop-Down-Menü **Add Resource to Cluster** (Ressource zum Cluster hinzufügen).
3. Klicken Sie auf das Drop-Down-Menü unter **Add Resource to Cluster** und wählen Sie den zu konfigurierenden Ressourcentyp.
4. Geben Sie die Ressourcenparameter für die hinzugefügte Ressource an. In [Anhang B, Parameter der Hochverfügbarkeitsressourcen](#) werden die Ressourcenparameter beschrieben.
5. Klicken Sie auf **Submit**. Durch den Klick auf **Submit** kehren Sie zur Ressourcenseite mit der **Resources**-Anzeige zurück, auf der nun neben anderen Ressourcen auch die neu hinzugefügte Ressource angezeigt wird.

Um eine vorhandene Ressource zu ändern, führen Sie die folgenden Schritte aus.

1. Klicken Sie auf der **luci Resources**-Seite auf den Namen der Ressource, die geändert werden soll. Daraufhin werden die Parameter für diese Ressource angezeigt.
2. Bearbeiten Sie die Ressourcenparameter.
3. Klicken Sie auf **Apply**.

Um eine vorhandene Ressource zu löschen, führen Sie die folgenden Schritte aus.

1. Markieren Sie auf der **luci Resources**-Seite die Auswahlkästchen all jener Ressourcen, die Sie löschen möchten.
2. Klicken Sie auf **Delete**.

3.9. Hinzufügen eines Cluster-Dienstes zum Cluster

Um einen Cluster-Dienst zum Cluster hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Sie können auf der clusterspezifischen Seite Dienste für diesen Cluster hinzufügen, indem Sie auf **Service Groups** oben in der Cluster-Ansicht klicken. Dadurch werden die Dienste angezeigt, die für diesen Cluster konfiguriert wurden. (Auf der **Service Groups**-Seite können Sie einen Dienst auch starten, stoppen und deaktivieren, wie in [Abschnitt 4.4, „Verwaltung von Hochverfügbarkeitsdiensten“](#) beschrieben.)
2. Klicken Sie auf **Add**. Dadurch erscheint das Dialogfeld **Add Service to Cluster** (Dienst zu Cluster hinzufügen).
3. Geben Sie im Dialogfeld **Add Service to Cluster** den Namen des Dienstes im Textfeld **Service name** ein.



Anmerkung

Der Name sollte aussagekräftig genug sein, um den Dienst klar von anderen Diensten im Cluster unterscheiden zu können.

4. Markieren Sie das Auswahlkästchen **Automatically start this service** (Diesen Dienst automatisch starten), falls Sie möchten, dass dieser Dienst beim Start des Clusters ebenfalls automatisch gestartet wird. Wird dieses Auswahlkästchen *nicht* markiert, muss der Dienst jedes Mal manuell gestartet werden, wenn der Cluster vom "Gestoppt"-Status wieder hochgefahren wird.
5. Markieren Sie das Auswahlkästchen **Run exclusive**, um die Richtlinie anzuwenden, nach der ein Dienst ausschließlich auf Knoten läuft, auf denen kein anderer Dienst ausgeführt wird.
6. Falls Sie Ausfallsicherungs-Domains für den Cluster konfiguriert haben, können Sie das Drop-Down-Menü des **Failover domain**-Parameters nutzen, um eine Ausfallsicherungs-Domain für diesen Dienst auszuwählen. Informationen über die Konfiguration von Ausfallsicherungs-Domains finden Sie in [Abschnitt 3.7, „Konfiguration einer Ausfallsicherungs-Domain“](#).
7. Verwenden Sie die Drop-Down-Liste **Recovery policy** (Richtlinie zur Wiederherstellung), um eine

Richtlinie zur Wiederherstellung des Dienstes festzulegen. Mögliche Optionen für den Dienst sind **Relocate** (Verlegung), **Restart** (Neustart), **Restart-Disable** (Neustart-Deaktivierung) oder **Disable** (Deaktivierung).

Wird die **Restart**-Option ausgewählt, so versucht das System einen Neustart des ausgefallenen Dienstes, bevor der Dienst verlegt wird. Wird die **Restart-Disable**-Option ausgewählt, versucht das System einen Neustart des ausgefallenen Dienstes an demselben Standort. Scheitert dieser Versuch, wird der Dienst deaktiviert, statt auf einen anderen Host im Cluster verlegt zu werden.

Falls Sie **Restart** oder **Restart-Disable** als Wiederherstellungsrichtlinie für diesen Dienst auswählen, können Sie die maximale Anzahl an Neustartfehlschlägen festlegen, bevor der Dienst verlegt oder deaktiviert wird, sowie die Zeitspanne in Sekunden, nach der ein Neustart nicht weiter versucht werden soll.

8. Um eine Ressource zum Dienst hinzuzufügen, klicken Sie auf **Add resource**. Durch den Klick auf **Add resource** wird ein Drop-Down-Menü angezeigt, aus dem Sie eine vorhandene globale Ressource oder eine vorhandene lokale Ressource, die *nur* diesem Dienst zur Verfügung steht, hinzufügen können.
 - ▶ Um eine vorhandene globale Ressource hinzuzufügen, klicken Sie im Drop-Down-Menü **Add Resource Service** (Ressource zu Dienst hinzufügen) auf den Namen der vorhandenen Ressource. Daraufhin wird auf der **Service Groups**-Seite für den Dienst, den Sie gerade konfigurieren, die Ressource und ihre Parameter angezeigt. Informationen über das Hinzufügen oder Verändern von globalen Ressourcen finden Sie in [Abschnitt 3.8, „Konfiguration von globalen Cluster-Eigenschaften“](#).
 - ▶ Um eine neue Ressource hinzuzufügen, die nur diesem Dienst zur Verfügung steht, wählen Sie den zu konfigurierenden Ressourcentyp aus dem Drop-Down-Menü **Add a resource** und geben Sie die Ressourcenparameter für die hinzuzufügende Ressource an. In [Anhang B, Parameter der Hochverfügbarkeitsressourcen](#) werden die Ressourcenparameter beschrieben.
 - ▶ Wenn Sie eine Ressource zu einem Dienst hinzufügen - egal, ob es sich dabei um eine vorhandene globale Ressource oder um eine nur für diesen Dienst verfügbare Ressource handelt - können Sie festlegen, ob diese Ressource ein **Unabhängiger Unterbaum** oder eine **Nicht-kritische Ressource** sein soll.

Wenn Sie festlegen, dass eine Ressource ein unabhängiger Unterbaum sein soll, wird im Falle eines Ausfalls dieser Ressource nur diese Ressource neu gestartet (statt des gesamten Dienstes), bevor das System die normale Wiederherstellung versucht. Sie können die maximale Anzahl der zu versuchenden Neustarts für diese Ressource auf einem Knoten festlegen, bevor die Wiederherstellungsrichtlinie für diesen Dienst zur Anwendung kommt. Sie können auch eine Zeitspanne festlegen, nach der das System die Wiederherstellungsrichtlinie für den Dienst anwendet.

Wenn Sie festlegen, dass die Ressource eine nicht-kritische Ressource ist, wird im Falle eines Ausfalls dieser Ressource nur diese Ressource neu gestartet, und falls die Ressource weiterhin fehlschlägt, wird nur diese Ressource deaktiviert (statt des gesamten Dienstes). Sie können die maximale Anzahl der zu versuchenden Neustarts für diese Ressource auf einem Knoten festlegen, bevor die Ressource deaktiviert wird. Sie können auch eine Zeitspanne festlegen, nach der das System die Ressource deaktiviert.

9. Falls Sie eine Kindressource zu der von Ihnen definierten Ressource hinzufügen möchten, klicken Sie auf **Add a child resource** (Kindressource hinzufügen). Durch den Klick auf **Add a child resource** wird das Drop-Down-Menü **Add Resource To Service** angezeigt, aus dem Sie eine vorhandene globale Ressource oder eine neue lokale Ressource, die nur diesem Dienst zur Verfügung steht, hinzufügen können. Je nach Bedarf können Sie weitere Kindressourcen zur Ihrer Ressource hinzufügen.



Anmerkung

Falls Sie eine Samba-Dienstressource hinzufügen, fügen Sie diese direkt zum Dienst hinzu, *nicht* als Kind einer anderen Ressource.

10. Wenn Sie damit fertig sind, Ressourcen zum Dienst und ggf. Kindressourcen zu den Ressourcen hinzuzufügen, klicken Sie auf **Submit**. Durch einen Klick auf **Submit** kehren Sie zur **Service**

Groups-Seite zurück, auf der neben den anderen Diensten nun auch der neu hinzugefügte Dienst angezeigt wird.



Anmerkung

Um zu überprüfen, ob die in einem Cluster-Dienst verwendete IP-Dienstressource existiert, müssen Sie den `/sbin/ip addr list`-Befehl auf einem Cluster-Knoten ausführen. Nachfolgend sehen Sie eine Ausgabe des `/sbin/ip addr list`-Befehls, der auf einem Knoten mit einem Cluster-Dienst ausgeführt wurde:

```
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
```

Um einen vorhandenen Dienst zu ändern, führen Sie die folgenden Schritte aus.

1. Klicken Sie im **luci Service Groups**-Dialogfeld auf den Namen des Dienstes, der geändert werden soll. Daraufhin werden die Parameter und Ressourcen angezeigt, die für diesen Dienst konfiguriert wurden.
2. Bearbeiten Sie die Dienstparameter.
3. Klicken Sie auf **Submit**.

Um einen vorhandenen Dienst zu löschen, führen Sie die folgenden Schritte aus.

1. Markieren Sie auf der **luci Service Groups**-Seite die Auswahlkästchen all jener Dienste, die Sie löschen möchten.
2. Klicken Sie auf **Delete**.

Kapitel 4. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga

Dieses Kapitel erläutert die verschiedenen administrativen Aufgaben zur Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons und umfasst die folgenden Abschnitte:

- ▶ [Abschnitt 4.1, „Hinzufügen eines vorhandenen Clusters zur luci-Oberfläche“](#)
- ▶ [Abschnitt 4.2, „Verwaltung von Cluster-Knoten“](#)
- ▶ [Abschnitt 4.3, „Starten, Stoppen, Neustarten und Löschen von Clustern“](#)
- ▶ [Abschnitt 4.4, „Verwaltung von Hochverfügbarkeitsdiensten“](#)

4.1. Hinzufügen eines vorhandenen Clusters zur luci-Oberfläche

Wenn Sie bereits einen Hochverfügbarkeits-Add-On-Cluster erstellt hatten, können Sie diesen Cluster einfach zur **luci**-Oberfläche hinzufügen, damit Sie diesen Cluster mit **Conga** verwalten können.

Um einen bereits vorhandenen Cluster zur **luci**-Oberfläche hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Manage Clusters** (Cluster verwalten) aus dem Menü auf der linken Seite der **luci Homebase**-Seite. Der Bildschirm **Clusters** erscheint.
2. Klicken Sie auf **Add** (Hinzufügen). Der Bildschirm **Add Existing Cluster** (Vorhandenen Cluster hinzufügen) erscheint.
3. Geben Sie den Knoten-Hostnamen und das **ricci**-Passwort für einen beliebigen Knoten in dem vorhandenen Cluster an. Da jeder Knoten im Cluster sämtliche Konfigurationsinformationen des Clusters enthält, sollte dies genügend Informationen liefern, um den Cluster zur **luci**-Oberfläche hinzuzufügen.
4. Klicken Sie auf **Connect** (Verbinden). Der Bildschirm **Add Existing Cluster** (Vorhandenen Cluster hinzufügen) zeigt daraufhin den Cluster-Namen und die verbleibenden Knoten im Cluster.
5. Geben Sie die jeweiligen **ricci**-Passwörter für jeden Knoten im Cluster an, oder geben Sie ein Passwort an und wählen **Use same password for all nodes** (Dasselbe Passwort für alle Knoten im Cluster verwenden).
6. Klicken Sie auf **Add Cluster** (Cluster hinzufügen). Der bereits konfigurierte Cluster wird nun im Bildschirm **Manage Clusters** angezeigt.

4.2. Verwaltung von Cluster-Knoten

Dieser Abschnitt beschreibt, wie die folgenden Funktionen zur Knotenverwaltung mithilfe der **luci** Server-Komponente von **Conga** durchgeführt werden:

- ▶ [Abschnitt 4.2.1, „Einen Cluster-Knoten neu starten“](#)
- ▶ [Abschnitt 4.2.2, „Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen“](#)
- ▶ [Abschnitt 4.2.3, „Ein Mitglied zu einem laufenden Cluster hinzufügen“](#)
- ▶ [Abschnitt 4.2.4, „Ein Mitglied aus einem Cluster löschen“](#)

4.2.1. Einen Cluster-Knoten neu starten

Um einen Knoten in einem Cluster neu zu starten, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** (Knoten) oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homebase**-Seite auf den Cluster-Namen klicken.
2. Wählen Sie den neu zu startenden Knoten, indem Sie das Auswahlkästchen des gewünschten Knotens markieren.
3. Wählen Sie die **Reboot** (Neustart)-Funktion aus dem Menü oben auf der Seite. Dies veranlasst

den Knoten zu einem Neustart und es erscheint eine Meldung oben auf der Seite, die besagt, dass dieser Knoten derzeit neu gestartet wird.

4. Aktualisieren Sie die Seite, um den aktuellen Status des Knotens zu sehen.

Es ist auch möglich, mehrere Knoten gleichzeitig neu zu starten, indem Sie alle gewünschten Knoten auswählen und anschließend auf **Reboot** (Neustart) klicken.

4.2.2. Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen

Sie können die **luci** Server-Komponente von **Conga** dazu verwenden, um einen Knoten zum Verlassen eines aktiven Clusters zu veranlassen, indem Sie alle Cluster-Dienste auf diesem Knoten stoppen. Sie können die **luci** Server-Komponente von **Conga** auch dazu verwenden, um einen Knoten, der einen Cluster verlassen hat, wieder zum Eintreten in den Cluster zu veranlassen.

Wenn Sie einen Knoten zum Verlassen eines Clusters veranlassen, löscht dies nicht die Cluster-Konfigurationsinformationen auf diesem Knoten, und der Knoten erscheint nach wie vor in der Cluster-Knotenanzeige mit dem Vermerk **Not a cluster member** (Kein Cluster-Mitglied). Informationen über das vollständige Löschen eines Knotens aus der Cluster-Konfiguration finden Sie in [Abschnitt 4.2.4, „Ein Mitglied aus einem Cluster löschen“](#).

Um einen Knoten zum Verlassen eines Clusters zu veranlassen, führen Sie die folgenden Schritte aus. Dadurch wird die Cluster-Software in dem Knoten beendet. Indem Sie einen Knoten dazu veranlassen, einen Cluster zu verlassen, wird verhindert, dass dieser Knoten automatisch wieder dem Cluster beitrifft, wenn dieser neu startet.

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** (Knoten) oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homepage**-Seite auf den Cluster-Namen klicken.
2. Wählen Sie den Knoten, der den Cluster verlassen soll, indem Sie das Auswahlkästchen für diesen Knoten markieren.
3. Wählen Sie die Funktion **Leave Cluster** (Cluster verlassen) aus dem Menü oben auf der Seite. Daraufhin erscheint eine Meldung oben auf der Seite, die besagt, dass dieser Knoten gestoppt wird.
4. Aktualisieren Sie die Seite, um den aktuellen Status des Knotens zu sehen.

Es ist auch möglich, mehrere Knoten gleichzeitig zum Verlassen des Clusters zu veranlassen, indem Sie alle gewünschten Knoten auswählen und anschließend auf **Leave Cluster** klicken.

Um einen Knoten zum Wiedereintritt in den Cluster zu veranlassen, wählen Sie alle Knoten, die dem Cluster wieder beitreten sollen, indem Sie deren Auswahlkästchen markieren und klicken Sie anschließend auf **Join Cluster** (Cluster beitreten). Dies veranlasst die ausgewählten Knoten dazu, dem Cluster wieder beizutreten, und es erlaubt den ausgewählten Knoten, dem Cluster automatisch beizutreten, wenn dieser neu gestartet wird.

4.2.3. Ein Mitglied zu einem laufenden Cluster hinzufügen

Um ein Mitglied zu einem laufenden Cluster hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homepage**-Seite auf den Cluster-Namen klicken.
2. Klicken Sie auf **Add** (Hinzufügen). Durch einen Klick auf **Add** wird das Dialogfeld **Add Nodes To Cluster** (Knoten zu diesem Cluster hinzufügen) angezeigt.
3. Geben Sie in dem Textfeld **Node Hostname** den Knotennamen und im Textfeld **Password** das **ricci**-Passwort ein. Falls Sie einen anderen Port für den **ricci**-Agent als den Standard 11111 verwenden, können Sie diesen Parameter hier ändern.
4. Markieren Sie das Auswahlkästchen **Enable Shared Storage Support** (Unterstützung für gemeinsam verwendeten Speicher aktivieren), falls geclusterter Speicher erforderlich ist, um die

Pakete herunterzuladen, die Unterstützung für geclusterten Speicher hinzufügen und um geclustertes LVM zu aktivieren. Sie sollten dies nur dann auswählen, wenn Sie Zugriff auf das Resilient Storage Add-On oder das Scalable File System Add-On haben.

5. Falls Sie weitere Knoten hinzufügen möchten, klicken Sie auf **Add Another Node** (Weiteren Knoten hinzufügen) und geben Sie den Knotennamen und das Passwort für jeden weiteren Knoten ein.
6. Klicken Sie auf **Add Nodes** (Knoten hinzufügen). Ein Klick auf **Add Nodes** löst die folgenden Aktionen aus:
 - a. Falls Sie **Download Packages** (Pakete herunterladen) ausgewählt haben, werden die Cluster-Software-Pakete auf die Knoten heruntergeladen.
 - b. Cluster-Software wird auf den Knoten installiert (bzw. es wird überprüft, ob die richtigen Software-Pakete installiert sind).
 - c. Die Cluster-Konfigurationsdatei wird aktualisiert und an jeden Knoten im Cluster weitergereicht — einschließlich dem hinzugefügten Knoten.
 - d. Der hinzugefügte Knoten tritt dem Cluster bei.

Die Seite **Nodes** erscheint mit einer Meldung, die besagt, dass der Knoten derzeit zum Cluster hinzugefügt wird. Aktualisieren Sie die Seite, um den aktuellen Status zu sehen.

7. Sobald der Vorgang zum Hinzufügen eines Knotens abgeschlossen ist, klicken Sie auf den Knotennamen des neu hinzugefügten Knotens, um das Fencing für diesen Knoten wie in [Abschnitt 3.5, „Konfiguration von Fencing-Geräten“](#) beschrieben zu konfigurieren.

4.2.4. Ein Mitglied aus einem Cluster löschen

Um ein Mitglied aus einem vorhandenen, derzeit laufenden Cluster zu löschen, folgen Sie den Schritten in diesem Abschnitt. Beachten Sie, dass vor dem Löschen von Knoten diese zunächst gestoppt werden müssen, es sei denn, Sie löschen alle Knoten im Cluster gleichzeitig.

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homepage**-Seite auf den Cluster-Namen klicken.



Anmerkung

Überspringen Sie den nächsten Schritt, um es Diensten zu ermöglichen, selbst auf einen anderen Knoten auszuweichen, wenn ihr Knoten gelöscht wird.

2. Deaktivieren oder Verlegen Sie jeden Dienst, der auf dem zu löschenden Knoten läuft. Informationen über das Deaktivieren oder Verlegen von Diensten finden Sie in [Abschnitt 4.4, „Verwaltung von Hochverfügbarkeitsdiensten“](#).
3. Wählen Sie den bzw. die zu löschenden Knoten.
4. Klicken Sie auf **Delete** (Löschen). Die Seite **Nodes** zeigt an, dass der Knoten derzeit gelöscht wird. Aktualisieren Sie die Seite, um den aktuellen Status zu sehen.

4.3. Starten, Stoppen, Neustarten und Löschen von Clustern

Sie können einen Cluster starten, stoppen und neu starten, indem Sie diese Aktionen auf den einzelnen Knoten im Cluster ausführen. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt.

Um einen Cluster zu stoppen, führen Sie die folgenden Schritte aus. Dadurch wird die Cluster-Software in den Knoten beendet, allerdings verbleibt die Cluster-Konfigurationsinformationen auf diesen Knoten und sie erscheinen nach wie vor in der Cluster-Knotenanzeige mit dem Vermerk **Not a cluster member** (Kein Cluster-Mitglied).

1. Wählen Sie alle Knoten im Cluster, indem Sie das Auswahlkästchen neben jedem Knoten markieren.

2. Wählen Sie die Funktion **Leave Cluster** (Cluster verlassen) aus dem Menü oben auf der Seite. Daraufhin erscheint eine Meldung oben auf der Seite, die besagt, dass jeder Knoten gestoppt wird.
3. Aktualisieren Sie die Seite, um den aktuellen Status der Knoten zu sehen.

Um einen Cluster zu starten, führen Sie die folgenden Schritte aus:

1. Wählen Sie alle Knoten im Cluster, indem Sie das Auswahlkästchen neben jedem Knoten markieren.
2. Wählen Sie die Funktion **Join Cluster** (Cluster beitreten) aus dem Menü oben auf der Seite.
3. Aktualisieren Sie die Seite, um den aktuellen Status der Knoten zu sehen.

Um einen laufenden Cluster neu zu starten, stoppen Sie zunächst alle Knoten im Cluster und starten anschließend wieder alle Knoten im Cluster, wie oben beschrieben.

Um einen Cluster vollständig von der **luci**-Oberfläche zu löschen, führen Sie die folgenden Schritte aus. Dadurch werden die Cluster-Konfigurationsinformationen von den Knoten gelöscht und diese aus der Cluster-Ansicht entfernt.



Wichtig

Das Löschen eines Clusters ist eine destruktive Operation, die nicht wieder rückgängig gemacht werden kann. Um einen Cluster nach dessen Löschung wiederherzustellen, müssen Sie den Cluster von Grund auf neu erstellen und neu definieren.

1. Wählen Sie alle Knoten im Cluster, indem Sie das Auswahlkästchen neben jedem Knoten markieren.
2. Wählen Sie die Funktion **Delete** (Löschen) aus dem Menü oben auf der Seite.

4.4. Verwaltung von Hochverfügbarkeitsdiensten

Zusätzlich zum Hinzufügen und Ändern eines Dienstes, wie in [Abschnitt 3.9 „Hinzufügen eines Cluster-Dienstes zum Cluster“](#) beschrieben, können Sie die folgenden Verwaltungsfunktionen für Hochverfügbarkeitsdienste über die **luci** Server-Komponente von **Conga** ausführen:

- ▶ Starten eines Dienstes
- ▶ Neustarten eines Dienstes
- ▶ Deaktivieren eines Dienstes
- ▶ Löschen eines Dienstes
- ▶ Verlegen eines Dienstes

Sie können auf der clusterspezifischen Seite Dienste für diesen Cluster verwalten, indem Sie auf **Service Groups** (Dienstgruppen) oben in der Cluster-Ansicht klicken. Dadurch werden die Dienste angezeigt, die für diesen Cluster konfiguriert wurden.

- ▶ Starten eines Dienstes — Um Dienste zu starten, die derzeit nicht ausgeführt werden, wählen Sie die gewünschten Dienste aus, indem Sie deren Auswahlkästchen markieren, und klicken Sie anschließend auf **Start**.
- ▶ Neustart eines Dienstes — Um Dienste neu zu starten, die derzeit ausgeführt werden, wählen Sie die gewünschten Dienste aus, indem Sie deren Auswahlkästchen markieren, und klicken Sie anschließend auf **Restart** (Neustart).
- ▶ Deaktivieren eines Dienstes — Um Dienste zu deaktivieren, die derzeit ausgeführt werden, wählen Sie die gewünschten Dienste aus, indem Sie deren Auswahlkästchen markieren, und klicken Sie anschließend auf **Disable** (Deaktivieren).
- ▶ Löschen eines Dienstes — Um Dienste zu löschen, die derzeit nicht ausgeführt werden, wählen Sie die gewünschten Dienste aus, indem Sie deren Auswahlkästchen markieren, und klicken Sie

anschließend auf **Delete** (Löschen).

- Verlegen eines Dienstes — Um einen laufenden Dienst zu verlegen, klicken Sie in der Dienste-Seite auf den Namen des gewünschten Dienstes. Dadurch wird die Dienst-Konfigurationsseite für diesen Dienst angezeigt, der Sie unter anderem entnehmen können, auf welchem Knoten der Dienst derzeit läuft.

Wählen Sie aus der Auswahlliste **Start on node . . .** (Starten auf Knoten...) denjenigen Knoten, auf den Sie diesen Dienst verlegen möchten, und klicken Sie anschließend auf das **Start**-Symbol. Es erscheint eine Meldung oben auf der Seite, die besagt, dass dieser Knoten derzeit gestartet wird. Sie müssen ggf. die Seite neu laden, um schließlich die neue Meldung zu erhalten, dass der Dienst nun auf dem von Ihnen ausgewählten Knoten ausgeführt wird.



Anmerkung

Sie können auch einen einzelnen Dienst starten, neu starten oder löschen, indem Sie auf der **Services**-Seite auf den Namen des Dienstes klicken. Dadurch wird die Dienst-Konfigurationsseite angezeigt. Oben rechts auf der Dienst-Konfigurationsseite sehen Sie dieselben Symbole für **Start**, **Restart**, **Disable** und **Delete**.

Kapitel 5. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem `ccs`-Befehl

Ab der Red Hat Enterprise Linux 6.1 Release bietet das Red Hat Hochverfügbarkeits-Add-On Unterstützung für den `ccs`-Cluster-Konfigurationsbefehl. Der `ccs`-Befehl ermöglicht es einem Administrator, die `cluster.conf`-Cluster-Konfigurationsdatei zu erstellen, zu bearbeiten, oder einzusehen. Sie können den `ccs`-Befehl verwenden, um eine Cluster-Konfigurationsdatei auf einem lokalen System oder auf einem entfernten Knoten zu konfigurieren. Mithilfe des `ccs`-Befehls kann ein Administrator zudem die Cluster-Dienste auf einem oder allen Knoten in einem konfigurierten Cluster starten oder stoppen.

Dieses Kapitel beschreibt die Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software mithilfe des `ccs`-Befehls. Informationen über die Verwendung des `ccs`-Befehls zur Verwaltung eines laufenden Clusters finden Sie in [Kapitel 6, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit `ccs`](#).

Dieses Kapitel umfasst die folgenden Abschnitte:

- ▶ [Abschnitt 5.1, „Überblick über operationale Aspekte“](#)
- ▶ [Abschnitt 5.2, „Konfigurationsaufgaben“](#)
- ▶ [Abschnitt 5.3, „Starten von `ricci`“](#)
- ▶ [Abschnitt 5.4, „Erstellen eines Clusters“](#)
- ▶ [Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“](#)
- ▶ [Abschnitt 5.6, „Konfigurieren von Fencing-Geräten für Cluster-Mitglieder“](#)
- ▶ [Abschnitt 5.7, „Konfigurieren einer Ausfallsicherungs-Domain“](#)
- ▶ [Abschnitt 5.8, „Konfigurieren von globalen Cluster-Ressourcen“](#)
- ▶ [Abschnitt 5.9, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#)
- ▶ [Abschnitt 5.10, „Konfigurieren einer Quorum-Platte“](#)
- ▶ [Abschnitt 5.11, „Sonstige Cluster-Konfiguration“](#)
- ▶ [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#)



Wichtig

Stellen Sie sicher, dass Ihr Deployment des Red Hat Hochverfügbarkeits-Add-Ons Ihren Anforderungen gerecht wird und unterstützt werden kann. Beratschlagen Sie sich dazu ggf. mit einem autorisierten Red Hat Vertreter, um Ihre Konfiguration vor dem Deployment zu verifizieren. Berücksichtigen Sie zudem eine gewisse Zeit für einen Burn-In-Test, um die Konfiguration auf mögliche Ausfälle zu überprüfen.



Wichtig

Dieses Kapitel verweist auf häufig verwendete `cluster.conf`-Elemente und -Parameter. Eine vollständige Liste samt Beschreibung aller `cluster.conf`-Elemente und -Attribute finden Sie im Cluster-Schema unter `/usr/share/cluster/cluster.rng` und dem annotierten Schema unter `/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html` (zum Beispiel `/usr/share/doc/cman-3.0.12/cluster_conf.html`).

5.1. Überblick über operationale Aspekte

Dieser Abschnitt beschreibt die folgenden, allgemeinen operationalen Aspekte des `ccs`-Befehls zur Konfiguration eines Clusters:

- ▶ [Abschnitt 5.1.1, „Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System“](#)

- ▶ [Abschnitt 5.1.2, „Anzeigen der aktuellen Cluster-Konfiguration“](#)
- ▶ [Abschnitt 5.1.3, „Angaben des ricci-Passworts mit dem ccs-Befehl“](#)
- ▶ [Abschnitt 5.1.4, „Ändern von Cluster-Konfigurationskomponenten“](#)

5.1.1. Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System

Mithilfe des `ccs`-Befehls können Sie eine Cluster-Konfigurationsdatei auf einem Cluster-Knoten erstellen, oder Sie können eine Cluster-Konfigurationsdatei auf einem lokalen Dateisystem erstellen und diese Datei anschließend auf einen Host in einem Cluster übertragen. Dies ermöglicht Ihnen, auf einer lokalen Maschine an der Datei zu arbeiten, diese unter Versionskontrolle zu verwalten, oder sie anderweitig je nach Bedarf zu kennzeichnen. Der `ccs`-Befehl erfordert keine Root-Privilegien.

Wenn Sie mit dem `ccs`-Befehl eine Cluster-Konfigurationsdatei auf einem Cluster-Knoten erstellen und bearbeiten, nutzen Sie die `-h`-Option, um den Namen des Hosts anzugeben. Dieser Befehl erstellt und bearbeitet die `cluster.conf`-Datei auf dem Host:

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

Um eine Cluster-Konfigurationsdatei auf einem lokalen System zu erstellen und zu bearbeiten, nutzen Sie die `-f`-Option des `ccs`-Befehls, um den Namen der Konfigurationsdatei anzugeben, wenn Sie eine Cluster-Operation ausführen. Sie können diese Datei nach Belieben benennen.

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

Nachdem Sie die Datei lokal erstellt haben, können Sie sie mithilfe der `--setconf`-Option des `ccs`-Befehls auf einen Cluster-Knoten übertragen. Auf einer Host-Maschine im Cluster wird die Datei `cluster.conf` benannt und im `/etc/cluster`-Verzeichnis abgelegt.

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

Werfen Sie für weitere Informationen über die Verwendung der `--setconf`-Option des `ccs`-Befehls einen Blick auf [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#).

5.1.2. Anzeigen der aktuellen Cluster-Konfiguration

Dieses Kapitel beschreibt, wie Sie eine Cluster-Konfigurationsdatei erstellen können. Falls Sie sich die derzeitige Konfigurationsdatei für einen Cluster anzeigen lassen möchten, nutzen Sie den folgenden Befehl und spezifizieren dabei einen Knoten im Cluster als Host:

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

Falls Sie Ihre Cluster-Konfigurationsdatei auf einem lokalen System erstellen, können Sie die `-f`-Option anstelle der `-h`-Option angeben, wie in [Abschnitt 5.1.1, „Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System“](#) beschrieben.

5.1.3. Angaben des ricci-Passworts mit dem ccs-Befehl

Damit Sie den `ccs`-Befehl dazu nutzen können, Kopien der `cluster.conf`-Datei an die Knoten im Cluster zu verbreiten, ist es erforderlich, dass `ricci` auf den Cluster-Knoten installiert ist und läuft, wie in [Abschnitt 2.11, „Überlegungen zu ricci“](#) beschrieben. Die Verwendung von `ricci` erfordert ein Passwort, wenn Sie zum ersten Mal von einem bestimmten Rechner aus mit `ricci` interagieren.

Falls Sie auf der von Ihnen verwendeten Maschine noch kein Passwort für eine `ricci`-Instanz auf einer bestimmten Maschine angegeben haben, werden Sie zur Eingabe dieses Passworts aufgefordert, wenn der `ccs`-Befehl es benötigt. Alternativ können Sie die `-p`-Option verwenden, um ein `ricci`-Passwort auf der Befehlszeile anzugeben.

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


Wenn Sie die `cluster.conf`-Datei mithilfe der `--sync`-Option des `ccs`-Befehls an alle Knoten im Cluster verbreiten und Sie dabei ein `ricci`-Passwort im Befehl angeben, wird der `ccs`-Befehl dieses Passwort für jeden Knoten im Cluster verwenden. Falls Sie auf den einzelnen Knoten jedoch verschiedene `ricci`-Passwörter festlegen möchten, können Sie den `--setconf`-Befehl mit der `-p`-Option verwenden, um die Konfigurationsdatei nacheinander an alle Knoten einzeln zu verbreiten.

5.1.4. Ändern von Cluster-Konfigurationskomponenten

Verwenden Sie den `ccs`-Befehl, um Cluster-Komponenten und Ihre Parameter in der Cluster-Konfigurationsdatei zu konfigurieren. Wenn Sie eine Cluster-Komponente zur Datei hinzugefügt haben und die Parameter dieser Komponente später verändern möchten, müssen Sie die definierte Komponente entfernen und sie mit den geänderten Parametern wieder hinzufügen. In den einzelnen Abschnitten dieses Kapitels finden Sie Informationen darüber, wie Sie dies für die jeweiligen Komponenten erreichen.

Die Parameter der `cman`-Cluster-Komponente stellen eine Ausnahme von diesem Verfahren zur Änderung von Cluster-Komponenten dar. Um diese Parameter zu ändern, können Sie die `--setcman`-Option des `ccs`-Befehls verwenden und die neuen Parameter angeben.

5.2. Konfigurationsaufgaben

Die Konfiguration der Red Hat Hochverfügbarkeits-Add-On Software mit `ccs` umfasst die folgenden Schritte:

1. Stellen Sie sicher, dass `ricci` auf allen Knoten im Cluster ausgeführt wird. Siehe [Abschnitt 5.3, „Starten von ricci“](#).
2. Erstellen Sie einen Cluster. Siehe [Abschnitt 5.4, „Erstellen eines Clusters“](#).
3. Konfigurieren Sie Fencing-Geräte. Siehe [Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“](#).
4. Konfigurieren Sie das Fencing für die Cluster-Mitglieder. Siehe [Abschnitt 5.6, „Konfigurieren von Fencing-Geräten für Cluster-Mitglieder“](#).
5. Erstellen Sie Ausfallsicherungs-Domains. Siehe [Abschnitt 5.7, „Konfigurieren einer Ausfallsicherungs-Domain“](#).
6. Erstellen Sie Ressourcen. Siehe [Abschnitt 5.8, „Konfigurieren von globalen Cluster-Ressourcen“](#).
7. Erstellen Sie Cluster-Dienste. Siehe [Abschnitt 5.9, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#).
8. Konfigurieren Sie eine Quorum-Platte, falls nötig. Siehe [Abschnitt 5.10, „Konfigurieren einer Quorum-Platte“](#).
9. Konfigurieren Sie globale Cluster-Eigenschaften. Siehe [Abschnitt 5.11, „Sonstige Cluster-Konfiguration“](#).
10. Verbreiten Sie die Cluster-Konfigurationsdatei auf allen Cluster-Knoten. Siehe [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#).

5.3. Starten von ricci

Um Cluster-Konfigurationsdateien zu erstellen und auf den Knoten im Cluster zu verbreiten, muss der `ricci`-Dienst auf jedem Knoten laufen. Bevor Sie `ricci` starten, sollten Sie sich vergewissern, dass Sie Ihr System folgendermaßen konfiguriert haben:

1. Die IP-Ports auf Ihren Cluster-Knoten sind für `ricci` aktiviert. Für Informationen über das Aktivieren von IP-Ports auf Cluster-Knoten werfen Sie bitte einen Blick auf [Abschnitt 2.3.1, „Aktivieren von IP-Ports auf Cluster-Knoten“](#).
2. Der `ricci`-Dienst ist auf allen Knoten im Cluster installiert, und es wurde ein `ricci`-Passwort zugewiesen, wie in [Abschnitt 2.11, „Überlegungen zu ricci“](#) beschrieben.

Nachdem `ricci` auf jedem Knoten installiert und konfiguriert wurde, starten Sie den `ricci`-Dienst auf jedem Knoten:

```
# service ricci start
Starting ricci:
```

[OK]

5.4. Erstellen eines Clusters

Dieser Abschnitt beschreibt, wie Sie ein Gerüst für eine Cluster-Konfiguration ohne Fencing, Ausfallsicherungs-Domains und Hochverfügbarkeitsdiensten mithilfe des `ccs`-Befehls erstellen, bearbeiten und löschen können. Nachfolgende Abschnitte beschreiben, wie diese Teile der Konfiguration konfiguriert werden.

Um ein Gerüst für eine Cluster-Konfigurationsdatei anzulegen, erstellen und benennen Sie zunächst den Cluster und fügen Sie anschließend Knoten zum Cluster hinzu, wie im folgenden Beispielverfahren veranschaulicht:

1. Erstellen Sie eine Cluster-Konfigurationsdatei auf einem der Knoten im Cluster, indem Sie den `ccs`-Befehl mit dem `-h`-Parameter ausführen, um den Knoten zu spezifizieren, auf dem die Datei erstellt werden soll, und die `createcluster`-Option, um den Namen für den Cluster zu spezifizieren:

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

Zum Beispiel erzeugt der folgende Befehl eine Konfigurationsdatei auf `node-01.example.com` namens `mycluster`:

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

Der Cluster-Name darf nicht länger als 15 Zeichen sein.

Falls bereits eine `cluster.conf`-Datei auf dem von Ihnen spezifizierten Host existiert, wird dieser Befehl die vorhandene Datei ersetzen.

Wenn Sie eine Cluster-Konfigurationsdatei auf Ihrem lokalen System erstellen möchten, können Sie die `-f`-Option anstelle der `-h`-Option verwenden. Werfen Sie für weitere Informationen über das lokale Erstellen der Datei einen Blick auf [Abschnitt 5.1.1, „Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System“](#).

2. Um die Knoten zu konfigurieren, aus denen sich der Cluster zusammensetzt, führen Sie den folgenden Befehl für jeden Knoten im Cluster aus:

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

Beispielsweise fügen die folgenden drei Befehle die Knoten `node-01.example.com`, `node-02.example.com` und `node-03.example.com` zur Konfigurationsdatei auf `node-01.example.com` hinzu:

```
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
```

Um eine Liste der Knoten anzusehen, die für einen Cluster konfiguriert wurden, führen Sie den folgenden Befehl aus:

```
ccs -h host --ltnodes
```

[Beispiel 5.1, „cluster.conf-Datei nach Hinzufügen von drei Knoten“](#) zeigt eine `cluster.conf`-Konfigurationsdatei, nachdem Sie den Cluster `mycluster` erstellt haben, der die Knoten `node-01.example.com`, `node-02.example.com` und `node-03.example.com` enthält.

Beispiel 5.1. cluster.conf-Datei nach Hinzufügen von drei Knoten

```
<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>
```

Wenn Sie einen Knoten zum Cluster hinzufügen, können Sie die Anzahl der Stimmen festlegen, über die der Knoten verfügt, und anhand derer bestimmt wird, ob ein Quorum vorliegt. Um die Anzahl der Stimmen für einen Cluster-Knoten zu spezifizieren, nutzen Sie folgenden Befehl:

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

Wenn Sie einen Knoten hinzufügen, weist **ccs** dem Knoten einen eindeutigen, ganzzahligen Wert zu, der als Knotenkennung dient. Falls Sie die Knotenkennung bei der Erstellung des Knotens manuell festlegen möchten, verwenden Sie folgenden Befehl:

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

Um einen Knoten aus dem Cluster zu entfernen, führen Sie den folgenden Befehl aus:

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

Wenn Sie die Konfiguration aller Komponenten Ihres Clusters abgeschlossen haben, müssen Sie die Cluster-Konfigurationsdatei auf allen Knoten synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

5.5. Konfigurieren von Fencing-Geräten

Das Konfigurieren von Fencing-Geräten umfasst das Erstellen, Aktualisieren und Löschen von Fencing-Geräten für den Cluster. Sie müssen die Fencing-Geräte in einem Cluster erstellen und benennen, bevor Sie das Fencing für die Knoten im Cluster konfigurieren können. Werfen Sie für Informationen über das Konfigurieren von Fencing für die einzelnen Knoten im Cluster einen Blick auf [Abschnitt 5.6, „Konfigurieren von Fencing-Geräten für Cluster-Mitglieder“](#).

Bevor Sie Ihre Fencing-Geräte konfigurieren, sollten Sie ggf. einige der Eigenschaften für den Fencing-Daemon für Ihr System abweichend von den Standardwerten einstellen. Die Werte, die Sie für den Fencing-Daemon konfigurieren können, sind allgemeine Werte für den Cluster. Die allgemeinen Fencing-Eigenschaften für den Cluster, die Sie ggf. anpassen sollten, lassen sich wie folgt zusammenfassen:

- Der Parameter **post_fail_delay** (Verzögerung nach Ausfall) ist die Anzahl von Sekunden, die der Fencing-Daemon (**fenced**) wartet, bevor ein Knoten (ein Mitglied der Fencing-Domain) nach dessen

Ausfall abgegrenzt wird. Der Standardwert für **post_fail_delay** ist **0**. Dieser Wert kann je nach Cluster- und Netzwerkleistung angepasst werden.

Um einen Wert für den **post_fail_delay**-Parameter zu konfigurieren, führen Sie den folgenden Befehl aus:

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

- Der Parameter **post_join_delay** (Verzögerung nach Beitritt) ist die Anzahl von Sekunden, die der Fencing-Daemon (**fenced**) wartet, bevor ein Knoten abgegrenzt wird, nachdem dieser der Fencing-Domain beigetreten ist. Der Standardwert für **post_join_delay** ist **3**. Ein typischer Wert für **post_join_delay** beträgt zwischen 20 und 30 Sekunden, kann sich jedoch je nach Cluster- und Netzwerkleistung unterscheiden.

Um einen Wert für den **post_join**-Parameter zu konfigurieren, führen Sie den folgenden Befehl aus:

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



Anmerkung

Weitere Informationen über die **post_join_delay** und **post_fail_delay** Parameter sowie weitere, konfigurierbare Fencing-Daemon-Eigenschaften finden Sie auf der fenced(8) Handbuchseite. Werfen Sie außerdem einen Blick auf das Cluster-Schema unter **/usr/share/cluster/cluster.rng** und das annotierte Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Um ein Fencing-Gerät für einen Cluster zu konfigurieren, führen Sie den folgenden Befehl aus:

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

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node1** ein apc-Fencing-Gerät namens **myfence** mit der IP-Adresse **apc_ip_example**, mit dem Login **login_example** und dem Passwort **password_example** zu erstellen, führen Sie den folgenden Befehl aus:

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

Das folgende Beispiel zeigt den **fencedevices**-Abschnitt der **cluster.conf**-Konfigurationsdatei, nachdem Sie dieses apc-Fencing-Gerät hinzugefügt haben:

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

Um eine Liste aller derzeit für Ihren Cluster konfigurierten Fencing-Geräte auszugeben, führen Sie den folgenden Befehl aus:

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

Um ein Fencing-Gerät aus Ihrer Cluster-Konfiguration zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmfencedev fence device name
```

Um beispielsweise ein Fencing-Gerät namens **myfence** aus der Cluster-Konfigurationsdatei auf dem

Cluster-Knoten **node1** zu löschen, führen Sie den folgenden Befehl aus:

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

Falls Sie die Parameter eines bereits konfigurierten Fencing-Geräts nachträglich ändern möchten, müssen Sie dieses Fencing-Gerät entfernen und mit den geänderten Parametern anschließend wieder hinzufügen.

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

5.6. Konfigurieren von Fencing-Geräten für Cluster-Mitglieder

Nachdem Sie die ersten Schritte zum Erstellen eines Clusters und zum Erstellen von Fencing-Geräten abgeschlossen haben, müssen Sie nun das Fencing für die Cluster-Knoten konfigurieren. Um das Fencing für die Knoten zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt. Beachten Sie, dass Sie das Fencing für jeden Knoten im Cluster konfigurieren müssen.

Diese Abschnitte dokumentieren die folgenden Verfahren:

- ▶ [Abschnitt 5.6.1, „Konfiguration eines einzelnen Power-Fencing-Geräts für einen Knoten“](#)
- ▶ [Abschnitt 5.6.2, „Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten“](#)
- ▶ [Abschnitt 5.6.3, „Konfiguration eines Backup-Fencing-Geräts“](#)
- ▶ [Abschnitt 5.6.4, „Konfiguration eines Knotens mit redundanter Stromversorgung“](#)
- ▶ [Abschnitt 5.6.5, „Entfernen von Fencing-Methoden und Fencing-Instanzen“](#)

5.6.1. Konfiguration eines einzelnen Power-Fencing-Geräts für einen Knoten

Verwenden Sie folgendes Verfahren, um einen Knoten mit einem einzelnen Power-Fencing-Gerät zu konfigurieren, das ein Fencing-Gerät namens **apc** verwendet, welches wiederum den **fence_apc**-Fencing-Agent verwendet.

1. Fügen Sie eine Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

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

Um beispielsweise eine Fencing-Methode namens **APC** für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie den folgenden Befehl aus:

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

2. Fügen Sie eine Fencing-Instanz für die Methode hinzu. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten:

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

Um beispielsweise eine Fencing-Instanz in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, die den APC Switch Power-Port 1 auf dem Fencing-Gerät namens **apc** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **APC** abzugrenzen, verwenden Sie folgenden Befehl:

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

Sie müssen für jeden Knoten im Cluster eine Fencing-Methode hinzufügen. Die folgenden Befehle

konfigurieren eine Fencing-Methode für jeden Knoten mit dem Methodennamen **APC**. Das Gerät für die Fencing-Methode spezifiziert **apc** als Gerätename, wobei es sich hierbei um ein Gerät handelt, das bereits vorher mit der **--addfencedev**-Option konfiguriert wurde, wie in [Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“](#) beschrieben. Jeder Knoten ist mit einer eindeutigen APC Switch Power-Port-Nummer konfiguriert: Die Port-Nummer für **node-01.example.com** ist **1**, die Port-Nummer für **node-02.example.com** ist **2**, und die Port-Nummer für **node-03.example.com** ist **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
```

[Beispiel 5.2, „cluster.conf nach Hinzufügen von Power-Fencing-Methoden“](#) zeigt eine **cluster.conf**-Konfigurationsdatei, nachdem Sie diese Fencing-Methoden und Instanzen zu jedem Knoten im Cluster hinzugefügt haben.

Beispiel 5.2. cluster.conf nach Hinzufügen von Power-Fencing-Methoden

```
<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>
```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

5.6.2. Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten

Wenn Sie andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing) zur

Abgrenzung eines Knotens verwenden, müssen Sie *Unfencing* für das Fencing-Gerät konfigurieren. Dadurch wird sichergestellt, dass ein abgegrenzter Knoten erst wieder aktiviert wird, nachdem er neu gestartet wurde. Wenn Sie Unfencing für einen Knoten konfigurieren, spezifizieren Sie ein Gerät als Spiegelbild des zugehörigen Fencing-Geräts für den Knoten, mit dem Unterschied, dass es die explizite Aktion **on** oder **enable** enthält.

Für weitere Informationen über das Unfencing von Knoten werfen Sie bitte einen Blick auf die **fence_node(8)** Handbuchseite.

Verwenden Sie folgendes Verfahren, um einen Knoten mit einem einzelnen Speicher-Fencing-Gerät zu konfigurieren, das ein Fencing-Gerät namens **sanswitch1** verwendet, welches wiederum den **fence_sanbox2**-Fencing-Agent verwendet.

1. Fügen Sie eine Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

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

Um beispielsweise eine Fencing-Methode namens **SAN** für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie den folgenden Befehl aus:

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

2. Fügen Sie eine Fencing-Instanz für die Methode hinzu. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten:

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

Um beispielsweise eine Fencing-Instanz in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, die den SAN Switch Power-Port 11 auf dem Fencing-Gerät namens **sanswitch1** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **SAN** abzugrenzen, verwenden Sie folgenden Befehl:

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

3. Um Unfencing für das Speicher-Fencing-Gerät auf diesem Knoten zu konfigurieren, führen Sie den folgenden Befehl aus:

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

Sie müssen für jeden Knoten im Cluster eine Fencing-Methode hinzufügen. Die folgenden Befehle konfigurieren eine Fencing-Methode für jeden Knoten mit dem Methodennamen **SAN**. Das Gerät für die Fencing-Methode spezifiziert **sanswitch** als Gerätenamen, wobei es sich hierbei um ein Gerät handelt, das bereits vorher mit der **--addfencedev**-Option konfiguriert wurde, wie in [Abschnitt 5.5](#), „[Konfigurieren von Fencing-Geräten](#)“ beschrieben. Jeder Knoten ist mit einer eindeutigen SAN physischen Port-Nummer konfiguriert: Die Port-Nummer für **node-01.example.com** ist **11**, die Port-Nummer für **node-02.example.com** ist **12**, und die Port-Nummer für **node-03.example.com** ist **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

```

[Beispiel 5.3 „cluster.conf nach Hinzufügen von Speicher-Fencing-Methoden“](#) zeigt eine **cluster.conf**-Konfigurationsdatei, nachdem Sie Fencing-Methoden, Fencing-Instanzen und Unfencing für jeden Knoten im Cluster hinzugefügt haben:

Beispiel 5.3. cluster.conf nach Hinzufügen von Speicher-Fencing-Methoden

```

<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>

```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-

Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

5.6.3. Konfiguration eines Backup-Fencing-Geräts

Sie können mehrere Fencing-Methoden für einen Knoten definieren. Falls die Abgrenzung mit der ersten Methode fehlschlägt, wird das System versuchen, den Knoten mithilfe der zweiten Methode abzugrenzen, gefolgt von jeglichen zusätzlichen konfigurierten Methoden. Um eine Backup-Fencing-Methode für einen Knoten zu konfigurieren, konfigurieren Sie zwei Methoden für einen Knoten und eine Fencing-Instanz für jede Methode.



Anmerkung

Die Reihenfolge, in der das System die konfigurierten Fencing-Methoden einsetzt, entspricht ihrer Reihenfolge in der Cluster-Konfigurationsdatei. Die erste Methode, die Sie mit dem **ccs**-Befehl konfigurieren, ist die primäre Fencing-Methode, die zweite von Ihnen konfigurierte Methode ist die Backup-Fencing-Methode. Um die Reihenfolge zu ändern, können Sie die primäre Fencing-Methode aus der Konfigurationsdatei löschen und diese Methode anschließend wieder hinzufügen.

Beachten Sie, dass Sie sich jederzeit eine Liste der aktuell für einen Knoten konfigurierten Fencing-Methoden und -Instanzen anzeigen lassen können, indem Sie den folgenden Befehl ausführen. Wenn Sie keinen bestimmten Knoten angeben, zeigt dieser Befehl die aktuell für alle Knoten konfigurierten Fencing-Methoden und -Instanzen an.

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

Verwenden Sie folgendes Verfahren, um einen Knoten mit einem einzelnen Power-Fencing-Gerät zu konfigurieren, das ein Fencing-Gerät namens **apc** verwendet, welches wiederum den **fence_apc**-Fencing-Agent verwendet, sowie ein Backup-Fencing-Gerät, das ein Fencing-Gerät namens **sanswitch1** verwendet, welches wiederum den **fence_sanbox2** Fencing-Agent verwendet. Da es sich beim **sanswitch1**-Gerät um ein Speicher-Fencing-Gerät handelt, müssen Sie für dieses Gerät zusätzlich Unfencing konfigurieren.

1. Fügen Sie eine primäre Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

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

Um beispielsweise eine Fencing-Methode namens **APC** als primäre Methode für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie folgenden Befehl aus:

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

2. Fügen Sie eine Fencing-Instanz für die primäre Methode hinzu. Sie müssen das zu verwendende Fencing-Gerät für den Knoten spezifizieren, sowie den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, und jegliche Optionen, die spezifisch für diesen Knoten sind:

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

Um beispielsweise eine Fencing-Instanz in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, die den APC Switch Power-Port 1 auf dem Fencing-Gerät namens **apc** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **APC** abzugrenzen, verwenden Sie folgenden Befehl:

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

3. Fügen Sie eine Backup-Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für

die Fencing-Methode an.

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

Um beispielsweise eine Backup-Fencing-Methode namens **SAN** für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie folgenden Befehl aus:

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

4. Fügen Sie eine Fencing-Instanz für die Backup-Methode hinzu. Sie müssen das zu verwendende Fencing-Gerät für den Knoten spezifizieren, sowie den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, und jegliche Optionen, die spezifisch für diesen Knoten sind:

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

Um beispielsweise eine Fencing-Instanz in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, die den SAN Switch Power-Port 11 auf dem Fencing-Gerät namens **sanswitch1** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **SAN** abzugrenzen, verwenden Sie folgenden Befehl:

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

5. Da es sich beim **sanswitch1**-Gerät um ein Speicher-Fencing-Gerät handelt, müssen Sie für dieses Gerät zusätzlich Unfencing konfigurieren.

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

Sie können nach Bedarf weitere Fencing-Methoden hinzufügen.

Dieses Verfahren konfiguriert ein Fencing-Gerät und ein Backup-Fencing-Gerät für einen Knoten im Cluster. Sie müssen das Fencing für die anderen Knoten im Cluster auf die gleiche Weise konfigurieren.

[Beispiel 5.4, „cluster.conf nach Hinzufügen von Backup-Fencing-Methoden“](#) zeigt eine **cluster.conf**-Konfigurationsdatei, nachdem Sie eine primäre Power-Fencing-Methode und eine Speicher-Backup-Fencing-Methode zu jedem Knoten im Cluster hinzugefügt haben.

Beispiel 5.4. cluster.conf nach Hinzufügen von Backup-Fencing-Methoden

```

<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>

```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.



Anmerkung

Die Reihenfolge, in der das System die konfigurierten Fencing-Methoden einsetzt, entspricht ihrer Reihenfolge in der Cluster-Konfigurationsdatei. Die erste Methode, die Sie konfigurieren, ist die primäre Fencing-Methode, die zweite von Ihnen konfigurierte Methode ist die Backup-Fencing-Methode. Um die Reihenfolge zu ändern, können Sie die primäre Fencing-Methode aus der Konfigurationsdatei löschen und diese Methode anschließend wieder hinzufügen.

5.6.4. Konfiguration eines Knotens mit redundanter Stromversorgung

Falls Ihr Cluster mit redundanter Stromversorgung für Ihre Knoten ausgestattet ist, vergewissern Sie sich, dass Ihr Fencing derart konfiguriert ist, dass Ihre Knoten bei der Abgrenzung vollständig abgeschaltet werden. Falls Sie jede Stromversorgung als separate Fencing-Methode konfigurieren, wird jede Stromversorgung separat abgegrenzt; die zweite Stromversorgung ermöglicht es dem System, weiterhin zu laufen, selbst wenn die erste Stromversorgung abgegrenzt ist, so dass das System selbst im Endeffekt nicht abgegrenzt wird. Um ein System mit dualer Stromversorgung zu konfigurieren, müssen Sie Ihre Fencing-Geräte so konfigurieren, dass beide Stromversorgungen abgeschaltet werden und somit auch das System vollständig abgeschaltet wird. Dazu ist es notwendig, dass Sie zwei Instanzen innerhalb einer einzelnen Fencing-Methode konfigurieren, und dass Sie für jede Instanz beide Fencing-Geräte mit dem **action**-Parameter **off** konfigurieren, bevor Sie anschließend jedes der Geräte mit dem **action**-Parameter **on** konfigurieren.

Um das Fencing für einen Knoten mit dualer Stromversorgung zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt.

1. Bevor Sie das Fencing für einen Knoten mit redundanter Stromversorgung konfigurieren können, müssen Sie jeden der Netzschalter als Fencing-Gerät für den Cluster konfigurieren. Informationen über die Konfiguration von Fencing-Geräten finden Sie in [Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“](#).

Um eine Liste aller derzeit für Ihren Cluster konfigurierten Fencing-Geräte auszugeben, führen Sie den folgenden Befehl aus:

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

2. Fügen Sie eine Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

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

Um beispielsweise eine Fencing-Methode namens **APC-dual** für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie den folgenden Befehl aus:

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

3. Fügen Sie eine Fencing-Instanz für die erste Stromversorgung zur Fencing-Methode hinzu. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten. Konfigurieren Sie an diesem Punkt den **action**-Parameter als **off**.

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

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** eine Fencing-Instanz zu konfigurieren, die den APC Switch Power Port 1 auf dem Fencing-Gerät namens **apc1** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **APC-dual** abzugrenzen und um den **action**-Parameter auf **off** zu setzen, führen Sie den folgenden Befehl aus:

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

- Fügen Sie eine Fencing-Instanz für die zweite Stromversorgung zur Fencing-Methode hinzu. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten. Konfigurieren Sie an diesem Punkt auch für diese Instanz den **action**-Parameter als **off**.

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

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** eine zweite Fencing-Instanz zu konfigurieren, die den APC Switch Power Port 1 auf dem Fencing-Gerät namens **apc2** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung derselben Methode wie für die erste Instanz namens **APC-dual** abzugrenzen und um den **action**-Parameter auf **off** zu setzen, führen Sie den folgenden Befehl aus:

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

- Fügen Sie nun eine weitere Fencing-Instanz für die erste Stromversorgung zur Fencing-Methode hinzu und konfigurieren Sie den **action**-Parameter auf **on**. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten, und spezifizieren Sie den **action**-Parameter **on**:

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

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** eine Fencing-Instanz zu konfigurieren, die den APC Switch Power Port 1 auf dem Fencing-Gerät namens **apc1** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **APC-dual** abzugrenzen und um den **action**-Parameter auf **on** zu setzen, führen Sie den folgenden Befehl aus:

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

- Fügen Sie eine weitere Fencing-Instanz für die zweite Stromversorgung zur Fencing-Methode hinzu und konfigurieren Sie den **action**-Parameter auf **on** für diese Instanz. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten, und spezifizieren Sie den **action**-Parameter **on**:

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

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** eine zweite Fencing-Instanz zu konfigurieren, die den APC Switch Power Port 1 auf dem Fencing-Gerät namens **apc2** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **APC-dual** abzugrenzen und um den **action**-Parameter auf **on** zu setzen, führen Sie den folgenden Befehl aus:

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

[Beispiel 5.5. „cluster.conf nach Hinzufügen von Fencing für duale Stromversorgung“](#) zeigt eine **cluster.conf**-Konfigurationsdatei, nachdem Sie Fencing für zwei Stromversorgungen für jeden Knoten im Cluster hinzugefügt haben.

Beispiel 5.5. cluster.conf nach Hinzufügen von Fencing für duale Stromversorgung

```

<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>

```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

5.6.5. Entfernen von Fencing-Methoden und Fencing-Instanzen

Um eine Fencing-Methode aus Ihrer Cluster-Konfiguration zu entfernen, führen Sie den folgenden Befehl aus:

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

Um beispielsweise eine Fencing-Methode namens **APC**, die Sie für **node01.example.com** konfiguriert hatten, aus der Cluster-Konfigurationsdatei auf dem Cluster-Knoten **node01.example.com** zu entfernen, führen Sie den folgenden Befehl aus:


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

Um alle Fencing-Instanzen eines Fencing-Geräts von einer Fencing-Methode zu entfernen, führen Sie den folgenden Befehl aus:

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

Um beispielsweise alle Instanzen des Fencing-Geräts namens **apc1** von der Methode namens **APC-dual1**, konfiguriert für **node01.example.com**, aus der Cluster-Konfigurationsdatei auf dem Cluster-Knoten **node01.example.com** zu entfernen, führen Sie den folgenden Befehl aus:

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

5.7. Konfigurieren einer Ausfallsicherungs-Domain

Eine Ausfallsicherungs-Domain ist eine benannte Teilmenge von Cluster-Knoten, die dazu berechtigt ist, einen Cluster-Dienst im Falle eines Knotenausfalls weiterzuführen. Eine Ausfallsicherungs-Domain kann die folgenden Charakteristiken haben:

- ▶ **Uneingeschränkt** — Ermöglicht Ihnen, eine Teilmenge bevorzugter Mitglieder zu spezifizieren, doch der dieser Domain zugewiesene Cluster-Dienst kann auf jedem verfügbaren Mitglied ausgeführt werden.
- ▶ **Eingeschränkt** — Ermöglicht Ihnen, die Mitglieder einzuschränken, auf denen ein bestimmter Cluster-Dienst laufen darf. Falls keines der Mitglieder in einer eingeschränkten Ausfallsicherungs-Domain verfügbar ist, kann der Cluster-Dienst nicht gestartet werden (weder manuell noch durch die Cluster-Software).
- ▶ **Ungeordnet** — Wenn ein Cluster-Dienst einer ungeordneten Ausfallsicherungs-Domain zugewiesen ist, wird das Mitglied, auf dem der Cluster-Dienst ausgeführt wird, ohne Berücksichtigung von Prioritäten aus den verfügbaren Mitgliedern der Ausfallsicherungs-Domain ausgewählt.
- ▶ **Geordnet** — Ermöglicht Ihnen, eine Prioritätsreihenfolge für die Mitglieder einer Ausfallsicherungs-Domain anzugeben. Das erste Mitglied in der Liste wird bevorzugt, gefolgt vom zweiten Mitglied in der Liste, usw.
- ▶ **Failback** — Ermöglicht Ihnen festzulegen, ob ein Dienst in der Ausfallsicherungs-Domain auf den Knoten zurückwechseln soll, auf dem er vor dessen Ausfall ursprünglich ausgeführt wurde. Das Konfigurieren dieser Charakteristik ist hilfreich in Situationen, in denen ein Knoten häufig ausfällt und Teil einer geordneten Ausfallsicherungs-Domain ist. In diesem Fall würde ein Dienst, der auf dem bevorzugten Knoten in einer Ausfallsicherungs-Domain läuft, möglicherweise wiederholt zwischen dem bevorzugten Knoten und einem anderen Knoten hin- und herwechseln, was beträchtliche Leistungseinbußen zur Folge hätte.



Anmerkung

Die Failback-Charakteristik greift nur, wenn die geordnete Ausfallsicherung konfiguriert ist.



Anmerkung

Eine Änderung der Ausfallsicherungs-Domain-Konfiguration hat keine Auswirkungen auf derzeit laufende Dienste.



Anmerkung

Ausfallsicherungs-Domains werden für den Betrieb *nicht* benötigt.

Standardmäßig sind Ausfallsicherungs-Domains uneingeschränkt und ungeordnet.

In einem Cluster mit mehreren Mitgliedern kann der Einsatz einer beschränkten Ausfallsicherungs-Domain Ihnen die Arbeit erleichtern. Denn um einen Cluster zum Ausführen eines Cluster-Dienstes (wie z.B. **httpd**) einzurichten, müssen Sie auf allen Cluster-Mitgliedern, die diesen Cluster-Dienst ausführen sollen, eine identische Konfiguration einrichten. Anstatt den gesamten Cluster zur Ausführung dieses Cluster-Dienstes einzurichten, müssen Sie somit nur die Mitglieder der beschränkten Ausfallsicherungs-Domain, die Sie mit diesem Cluster-Dienst verknüpfen möchten, entsprechend einrichten.



Anmerkung

Um ein bevorzugtes Mitglied zu konfigurieren, können Sie eine uneingeschränkte Ausfallsicherungs-Domain einrichten, die nur aus einem Cluster-Mitglied besteht. Dadurch läuft der Cluster-Dienst zwar hauptsächlich auf diesem einen Cluster-Mitglied (dem bevorzugten Mitglied), doch erlaubt es dem Cluster-Dienst gleichzeitig, im Falle eines Ausfalls auf einen beliebigen anderen Knoten zu wechseln.

Um eine Ausfallsicherungs-Domain zu konfigurieren, wenden Sie folgendes Verfahren an:

1. Um eine Ausfallsicherungs-Domain hinzuzufügen, führen Sie den folgenden Befehl aus:

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



Anmerkung

Der Name sollte aussagekräftig genug sein, um daraus im Vergleich zu anderen Namen im Cluster auf den Zweck schließen zu können.

Beispielsweise konfiguriert der folgende Befehl eine Ausfallsicherungs-Domain namens **example_pri** auf **node-01.example.com**, die uneingeschränkt und geordnet ist und Failback erlaubt:

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

2. Um einen Knoten zu einer Ausfallsicherungs-Domain hinzuzufügen, führen Sie den folgenden Befehl aus:

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

Um beispielsweise die Ausfallsicherungs-Domain **example_pri** in der Konfigurationsdatei auf **node-01.example.com** so zu konfigurieren, dass sie **node-01.example.com** mit der Priorität 1, **node-02.example.com** mit der Priorität 2 und **node-03.example.com** mit der Priorität 3 beinhaltet, führen Sie die folgenden Befehle aus:

```
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-01.example.com 3
```

Sie können sich mithilfe des folgenden Befehls eine Liste aller in einem Cluster konfigurierten Ausfallsicherungs-Domains und Ausfallsicherungs-Domain-Knoten anzeigen lassen:

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

Um eine Ausfallsicherungs-Domain zu entfernen, führen Sie den folgenden Befehl aus:

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

Um einen Knoten aus einer Ausfallsicherungs-Domain zu entfernen, führen Sie den folgenden Befehl aus:

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

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

5.8. Konfigurieren von globalen Cluster-Ressourcen

Sie können zwei Arten von Ressourcen konfigurieren:

- Global — Ressourcen, die jedem Dienst im Cluster zur Verfügung stehen.
- Dienst-spezifisch — Ressourcen, die nur einem Dienst zur Verfügung stehen.

Um eine Liste der derzeit konfigurierten Ressourcen und Dienste im Cluster zu sehen, führen Sie den folgenden Befehl aus:

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

Um eine globale Cluster-Ressource hinzuzufügen, führen Sie den folgenden Befehl aus. Sie können eine Ressource lokal für einen bestimmten Dienst hinzufügen, während Sie diesen Dienst konfigurieren, wie in [Abschnitt 5.9, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#) beschrieben.

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

Beispielsweise fügt der folgende Befehl eine globale Dateisystemressource zur Cluster-Konfigurationsdatei auf **node01.example.com** hinzu. Der Name der Ressource lautet **web_fs**, das Dateisystemgerät ist **/dev/sdd2**, der Einhängepunkt des Dateisystems ist **/var/www**, und der Dateisystemtyp ist **ext3**.

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

Werfen Sie für Informationen über die verfügbaren Ressourcentypen und Ressourcenoptionen bitte einen Blick auf [Anhang B, Parameter der Hochverfügbarkeitsressourcen](#).

Um eine globale Ressource zu löschen, führen Sie den folgenden Befehl aus:

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

Falls Sie die Parameter einer vorhandenen, globalen Ressource ändern müssen, können Sie die Ressourcen entfernen und sie erneut konfigurieren.

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

5.9. Hinzufügen eines Cluster-Dienstes zum Cluster

Um einen Cluster-Dienst in einem Cluster zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Fügen Sie mithilfe des folgenden Befehls einen Dienst zum Cluster hinzu:

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



Anmerkung

Der Name sollte aussagekräftig genug sein, um den Dienst klar von anderen Diensten im Cluster unterscheiden zu können.

Wenn Sie einen Dienst zur Cluster-Konfiguration hinzufügen, können Sie die folgenden Parameter konfigurieren:

- ▶ **autostart** — Legt fest, ob der Dienst beim Start des Clusters automatisch gestartet werden soll.
- ▶ **domain** — Legt eine Ausfallsicherungs-Domain fest (falls erforderlich).
- ▶ **exclusive** — Legt eine Richtlinie fest, gemäß der dieser Dienst ausschließlich auf Knoten ausgeführt werden darf, auf denen kein anderer Dienst läuft.
- ▶ **recovery** — Legt eine Richtlinie zur Wiederherstellung des Dienstes fest. Zu den Optionen gehören Neustart, Verlegung, Deaktivierung und Neustart/Deaktivierung des Dienstes. Weitere Informationen über die Wiederherstellungsrichtlinien für Dienste finden Sie in [Tabelle B.18, „Dienst“](#).

Um beispielsweise einen Dienst namens **example_apache** zur Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** hinzuzufügen, der die Ausfallsicherungs-Domain **example_pri** nutzt und die Wiederherstellungsrichtlinie **relocate** verwendet, führen Sie den folgenden Befehl aus:

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

2. Fügen Sie mithilfe des folgenden Befehls Ressourcen zu diesem Dienst hinzu:

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

Bestücken Sie den Dienst abhängig von dem Ressourcentyp, den Sie verwenden möchten, entweder mit globalen oder dienstspezifischen Ressourcen. Um eine globale Ressource hinzuzufügen, verwenden Sie die **--addsubservice**-Option von **ccs**. Um beispielsweise die globale Dateisystemressource namens **web_fs** zu dem Dienst namens **example_apache** in der Cluster-Konfigurationsdatei auf **node-01.example.com** hinzuzufügen, führen Sie den folgenden Befehl aus:

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

Um eine dienstspezifische Ressource zum Dienst hinzuzufügen, müssen Sie sämtliche Diensoptionen angeben. Falls Sie beispielsweise **web_fs** nicht bereits als globalen Dienst definiert haben, können Sie es mithilfe des folgenden Befehls als dienstspezifische Ressource hinzufügen:

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

3. Um einen untergeordneten Dienst zu diesem Dienst hinzuzufügen, verwenden Sie zudem die **--addsubservice**-Option des **ccs**-Befehls und geben dabei die Diensoptionen an.

Falls Sie Dienst innerhalb einer Baumstruktur von Abhängigkeiten hinzufügen müssen, verwenden Sie einen Doppelpunkt (":"), um Elemente voneinander zu trennen, und Klammern, um untergeordnete Dienste desselben Typs zu identifizieren. Das folgende Beispiel fügt einen dritten **nfscient**-Dienst als untergeordneten Dienst eines **nfscient**-Dienstes hinzu, der selbst ein untergeordneter Dienst eines **nfscient**-Dienstes ist, der selbst wiederum ein untergeordneter Dienst eines Dienstes namens **service_a** ist:

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

Anmerkung

Falls Sie eine Samba-Dienstressource hinzufügen, fügen Sie diese direkt zum Dienst hinzu, *nicht* einer anderen Ressource untergeordnet.

Anmerkung

Um zu überprüfen, ob die in einem Cluster-Dienst verwendete IP-Dienstressource existiert, müssen Sie den `/sbin/ip addr list`-Befehl auf einem Cluster-Knoten ausführen. Nachfolgend sehen Sie eine Ausgabe des `/sbin/ip addr list`-Befehls, der auf einem Knoten mit einem Cluster-Dienst ausgeführt wurde:

```
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
```

Um einen Dienst samt aller zugehörigen untergeordneten Dienste zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmsservice servicename
```

Führen Sie den folgenden Befehl aus, um einen untergeordneten Dienst zu entfernen:

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

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

5.10. Konfigurieren einer Quorum-Platte

Wichtig

Quorum-Plattenparameter und Heuristiken hängen von der jeweiligen Umgebung und ggf. besonderen Anforderungen ab. Um die Verwendung von Quorum-Plattenparametern und Heuristiken zu verstehen, werfen Sie einen Blick auf die `qdisk(5)`-Handbuchseite. Falls Sie Hilfe zum Verständnis oder zur Verwendung von Quorum-Platten benötigen, setzen Sie sich bitte mit einem autorisierten Red Hat Support-Vertreter in Verbindung.

Verwenden Sie den folgenden Befehl, um Ihr System zur Verwendung einer Quorum-Platte zu konfigurieren:

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

[Tabelle 5.1, „Quorum-Plattenoptionen“](#) fasst die Bedeutung der Quorum-Plattenoptionen zusammen, die Sie ggf. einstellen müssen. Eine vollständige Liste der Quorum-Plattenparameter finden Sie im Cluster-

Schema unter `/usr/share/cluster/cluster.rng` sowie im annotierten Schema unter `/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html`.

Tabelle 5.1. Quorum-Plattenoptionen

| Parameter | Beschreibung |
|------------------|---|
| interval | Die Häufigkeit von Lese-/Schreibzyklen in Sekunden. |
| votes | Die Anzahl der Stimmen, die der Quorum-Daemon an cman mitteilt, wenn eine Punktzahl erreicht wird, die hoch genug ist. |
| tko | Die Anzahl von Zyklen, die ein Knoten auslassen muss, bevor dieser für tot erklärt wird. |
| min_score | Die Mindestpunktzahl eines Knotens, bei der dieser noch als "lebendig" betrachtet wird. Falls dieser Wert weggelassen oder auf 0 gesetzt wird, so wird die Standardfunktion $\text{floor}((n+1)/2)$ verwendet, wobei n die Summe der Heuristik-Punktzahlen ist. Der Minimum Score Wert darf nie die Summe der Heuristik-Punktzahlen übersteigen, andernfalls wird die Quorum-Platte nicht verfügbar sein. |
| device | Das vom Quorum-Daemon verwendete Speichergerät. Das Gerät muss auf allen Knoten dasselbe sein. |
| label | Spezifiziert das Quorum-Platten-Label, das von dem mkqdisk -Dienstprogramm erstellt wurde. Wird dieses Feld verwendet, liest der Quorum-Daemon die <code>/proc/partitions</code> , sucht nach qdisk-Signaturen auf jedem gefundenen Blockgerät und vergleicht das Label mit dem angegebenen Label. Dies ist in Konfigurationen hilfreich, in denen der Name des Quorum-Geräts sich von Knoten zu Knoten unterscheidet. |

Verwenden Sie den folgenden Befehl, um die Heuristiken für eine Quorum-Platte zu konfigurieren:

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

[Tabelle 5.2. „Quorum-Plattenheuristiken“](#) fasst die Bedeutung der Quorum-Plattenheuristiken zusammen, die Sie ggf. einstellen müssen.

Tabelle 5.2. Quorum-Plattenheuristiken

| Parameter | Beschreibung |
|-----------------|--|
| program | Das Programm, das dazu verwendet wird zu bestimmen, ob diese Heuristik verfügbar ist. Dies kann alles sein, was durch <code>/bin/sh -c</code> ausgeführt werden kann. Ein Rückgabewert von 0 bedeutet eine erfolgreiche Durchführung, alles andere bedeutet ein Scheitern. Dieses Feld ist erforderlich. |
| interval | Die Zeitabstände (in Sekunden), in denen die Heuristik abgefragt wird. Das standardmäßige Intervall für jede Heuristik ist 2 Sekunden. |
| score | Das Gewicht dieser Heuristik. Seien Sie vorsichtig beim Festlegen des Gewichts für Heuristiken. Das standardmäßige Gewicht für jede Heuristik ist 1. |
| tko | Die Anzahl von aufeinander folgenden Fehlschlägen, bevor diese Heuristik für nicht verfügbar erklärt wird. |

Um eine Liste der Quorum-Plattenoptionen und Heuristiken einzusehen, die auf einem System konfiguriert sind, können Sie den folgenden Befehl ausführen:

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

Um eine Heuristik zu entfernen, die von einer Heuristikooption spezifiziert wird, können Sie den folgenden Befehl ausführen:

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

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.



Anmerkung

Durch das Synchronisieren und Aktivieren wird die aktualisierte Cluster-Konfigurationsdatei verbreitet und aktiviert. Damit die Quorum-Platte jedoch funktioniert, muss der Cluster neu gestartet werden (siehe [Abschnitt 6.2, „Starten und Stoppen eines Clusters“](#)).

5.11. Sonstige Cluster-Konfiguration

Dieser Abschnitt beschreibt die Verwendung des **ccs**-Befehls, um Folgendes zu konfigurieren:

- ▶ [Abschnitt 5.11.1, „Cluster-Konfigurationsversion“](#)
- ▶ [Abschnitt 5.11.2, „Multicast-Konfiguration“](#)
- ▶ [Abschnitt 5.11.3, „Konfiguration eines Zwei-Knoten-Clusters“](#)

Sie können den **ccs**-Befehl auch dazu verwenden, erweiterte Cluster-Konfigurationsparameter einzustellen, wie z.B. **totem**-Optionen, **d1m**-Optionen, **rm**-Optionen und **cman**-Optionen. Werfen Sie für Informationen über das Einstellen dieser Parameter einen Blick auf die **ccs(8)** Handbuchseite und das annotierte Cluster-Konfigurationsdatei-Schema unter `/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html`.

Um eine Liste der sonstigen Cluster-Parameter anzusehen, die für einen Cluster konfiguriert wurden, führen Sie den folgenden Befehl aus:

```
ccs -h host --lsmisc
```

5.11.1. Cluster-Konfigurationsversion

Eine Cluster-Konfigurationsdatei beinhaltet einen Konfigurationsversions-Wert. Der Konfigurationsversions-Wert wird standardmäßig auf **1** gesetzt, wenn Sie eine Cluster-Konfigurationsdatei erstellen, und wird jedes Mal automatisch erhöht, wenn Sie Ihre Cluster-Konfiguration ändern. Falls Sie jedoch einen abweichenden Wert angeben müssen, können Sie diesen mithilfe des folgenden Befehls angeben:

```
ccs -h host --setversion n
```

Sie können den aktuellen Konfigurationsversions-Wert auf einer vorhandenen Cluster-Konfigurationsdatei mit dem folgenden Befehl abrufen:

```
ccs -h host --getversion
```

Um den aktuellen Konfigurationsversions-Wert in der Cluster-Konfigurationsdatei auf jedem Knoten im Cluster um 1 zu erhöhen, führen Sie den folgenden Befehl aus:

```
ccs -h host --incversion
```

5.11.2. Multicast-Konfiguration

Falls Sie in der Cluster-Konfigurationsdatei keine Multicast-Adresse angeben, erstellt die Red Hat Hochverfügbarkeits-Add-On-Software eine Multicast-Adresse basierend auf der Cluster-ID. Es generiert die unteren 16 Bits der Adresse und fügt diese dem oberen Teil der Adresse an, abhängig davon, ob

das IP-Protokoll IPV4 oder IPV6 verwendet wird:

- ▶ Bei IPV4 — Die gebildete Adresse ist 239.192. plus die von der Red Hat Hochverfügbarkeits-Add-On-Software generierten unteren 16 Bits.
- ▶ Bei IPV6 — Die gebildete Adresse ist FF15:: plus die von der Red Hat Hochverfügbarkeits-Add-On-Software generierten unteren 16 Bits.



Anmerkung

Die Cluster-ID ist eine eindeutige Kennung, die `cman` für jeden Cluster generiert. Um die Cluster-ID einzusehen, führen Sie den Befehl `cman_tool status` auf einem Cluster-Knoten aus.

Mithilfe des folgenden Befehls können Sie manuell eine Multicast-Adresse in der Cluster-Konfigurationsdatei spezifizieren:

```
ccs -h host --setmulticast multicastaddress
```

Falls Sie eine Multicast-Adresse angeben, sollten Sie die 239.192.x.x Serien (oder FF15:: für IPv6) nutzen, die `cman` verwendet. Falls Sie eine Multicast-Adresse außerhalb dieses Bereichs verwenden, kann dies andernfalls zu unvorhergesehenem Verhalten führen. So könnte z.B. die Adresse 224.0.0.x (d.h. "Alle Hosts auf dem Netzwerk") unter Umständen von mancher Hardware nicht korrekt oder gar nicht geroutet werden.



Anmerkung

Falls Sie eine Multicast-Adresse angeben, überprüfen Sie die Konfiguration der Router, die von Cluster-Paketen durchquert werden. Manche Router brauchen eine lange Zeit zum Lernen von Adressen, was sich drastisch auf die Cluster-Leistung auswirken kann.

Um eine Multicast-Adresse aus einer Konfigurationsdatei zu entfernen, verwenden Sie die `--setmulticast`-Option von `ccs`, geben dabei aber keine Multicast-Adresse an:

```
ccs -h host --setmulticast
```

5.11.3. Konfiguration eines Zwei-Knoten-Clusters

Falls Sie einen Zwei-Knoten-Cluster konfigurieren, können Sie den folgenden Befehl ausführen, damit es einem einzelnen Knoten möglich ist, das Quorum zu erhalten (z.B. falls der andere Knoten ausfällt):

```
ccs -h host --setcman two_node=1 expected_votes=1
```

5.12. Verbreiten der Konfigurationsdatei auf den Cluster-Knoten

Nachdem Sie auf einem der Knoten im Cluster eine Cluster-Konfigurationsdatei erstellt oder bearbeitet haben, müssen Sie diese Datei auf alle Cluster-Knoten verbreiten und die Konfiguration aktivieren.

Verwenden Sie den folgenden Befehl, um eine Cluster-Konfigurationsdatei zu verbreiten und zu aktivieren:

```
ccs -h host --sync --activate
```

Um zu überprüfen, ob alle in der Cluster-Konfigurationsdatei des Hosts spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen, führen Sie den folgenden Befehl aus:

```
ccs -h host --checkconf
```

Falls Sie auf einem lokalen Knoten eine Cluster-Konfigurationsdatei erstellt oder bearbeitet haben, verwenden Sie den folgenden Befehl, um diese Datei an einen der Knoten im Cluster zu übertragen:

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

Um zu überprüfen, ob alle in der lokalen Datei spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen, führen Sie den folgenden Befehl aus:

```
ccs -f file --checkconf
```

Kapitel 6. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit ccs

Dieses Kapitel erläutert die verschiedenen administrativen Aufgaben zur Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mithilfe des `ccs`-Befehls, der ab der Red Hat Enterprise Linux 6.1 Release unterstützt wird. Dieses Kapitel umfasst die folgenden Abschnitte:

- ▶ [Abschnitt 6.1, „Verwaltung von Cluster-Knoten“](#)
- ▶ [Abschnitt 6.2, „Starten und Stoppen eines Clusters“](#)
- ▶ [Abschnitt 6.3, „Fehlerdiagnose und -behebung in einem Cluster“](#)

6.1. Verwaltung von Cluster-Knoten

Dieser Abschnitt beschreibt, wie die folgenden Funktionen zur Knotenverwaltung mithilfe des `ccs`-Befehls durchgeführt werden:

- ▶ [Abschnitt 6.1.1, „Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen“](#)
- ▶ [Abschnitt 6.1.2, „Ein Mitglied zu einem laufenden Cluster hinzufügen“](#)

6.1.1. Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen

Sie können den `ccs`-Befehl dazu verwenden, um einen Knoten zum Verlassen eines Clusters zu veranlassen, indem Sie alle Cluster-Dienste auf diesem Knoten stoppen. Wenn Sie einen Knoten zum Verlassen eines Clusters veranlassen, löscht dies nicht die Cluster-Konfigurationsinformationen auf diesem Knoten. Vielmehr wird dadurch verhindert, dass dieser Knoten automatisch wieder dem Cluster beitrifft, wenn dieser neu startet.

Um einen Knoten zum Verlassen eines Clusters zu veranlassen, führen Sie den folgenden Befehl aus, wodurch die Cluster-Dienste auf dem mit der `-h`-Option spezifizierten Knoten beendet werden.

```
ccs -h host --stop
```

Wenn Sie Cluster-Dienste auf einem Knoten stoppen, werden Dienste, die auf diesem Knoten laufen, auf andere Knoten verlegt.

Um einen Knoten vollständig aus der Cluster-Konfiguration zu löschen, verwenden Sie die `--rmnode`-Option des `ccs`-Befehls, wie in [Abschnitt 5.4, „Erstellen eines Clusters“](#) beschrieben.

Um einen Knoten zum Wiedereintritt in den Cluster zu veranlassen, führen Sie den folgenden Befehl aus, wodurch die Cluster-Dienste auf dem mit der `-h`-Option spezifizierten Knoten gestartet werden.

```
ccs -h host --start
```

6.1.2. Ein Mitglied zu einem laufenden Cluster hinzufügen

Um ein Mitglied zu einem laufenden Cluster hinzuzufügen, fügen Sie dem Cluster einen Knoten wie in [Abschnitt 5.4, „Erstellen eines Clusters“](#) beschrieben hinzu. Nachdem die Konfigurationsdatei aktualisiert wurde, verbreiten Sie diese an alle Knoten im Cluster und aktivieren Sie die neue Cluster-Konfigurationsdatei, wie in [Abschnitt 5.12, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“](#) beschrieben.

6.2. Starten und Stoppen eines Clusters

Sie können den `ccs`-Befehl dazu verwenden, um einen Cluster zu stoppen, indem Sie mithilfe des folgenden Befehls die Cluster-Dienste auf allen Knoten im Cluster stoppen:

```
ccs -h host --stopall
```

Sie können den **ccs**-Befehl dazu verwenden, um einen derzeit nicht laufenden Cluster zu starten, indem Sie mithilfe des folgenden Befehls die Cluster-Dienste auf allen Knoten im Cluster starten:

```
ccs -h host --startall
```

6.3. Fehlerdiagnose und -behebung in einem Cluster

Für Informationen über die Diagnose und Behebung von Problemen in einem Cluster, siehe [Kapitel 9. Fehlerdiagnose und -behebung in einem Cluster](#). Es gibt zudem einige einfache Tests, die Sie mit dem **ccs**-Befehl vornehmen können.

Um zu überprüfen, ob alle in der Cluster-Konfigurationsdatei des Hosts spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen, führen Sie den folgenden Befehl aus:

```
ccs -h host --checkconf
```

Falls Sie eine Konfigurationsdatei auf einem lokalen Knoten bearbeitet oder erstellt haben, können Sie überprüfen, ob alle in der lokalen Datei spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen, indem Sie den folgenden Befehl ausführen:

```
ccs -f file --checkconf
```

Kapitel 7. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools

Dieses Kapitel erläutert, wie Sie die Red Hat Hochverfügbarkeits-Add-On-Software durch direktes Bearbeiten der Cluster-Konfigurationsdatei (`/etc/cluster/cluster.conf`) und unter Verwendung von Befehlszeilen-Tools konfigurieren können. Das Kapitel zeigt Verfahren zum abschnittswisen Erstellen einer Konfigurationsdatei, ausgehend von einer bereitgestellten Beispieldatei. Alternativ zur Bearbeitung der hier bereitgestellten Beispieldatei können Sie auch das Gerüst für die Konfigurationsdatei von der `cluster.conf`-Handbuchseite kopieren, allerdings lassen sich die in den nachfolgenden Verfahren angegebenen Informationen dann nicht unbedingt auf diesen Fall übertragen. Es gibt verschiedene Wege zum Erstellen und Konfigurieren einer Cluster-Konfigurationsdatei; dieses Kapitel beschreibt die Verfahren zum abschnittswisen Erstellen einer Konfigurationsdatei. Bedenken Sie zudem, dass dieses Kapitel nur ein Ausgangspunkt zur Entwicklung einer Konfigurationsdatei sein kann und Sie Ihre Konfigurationsdatei ggf. weiter auf Ihre Clustering-Bedürfnisse anpassen müssen.

Dieses Kapitel umfasst die folgenden Abschnitte:

- ▶ [Abschnitt 7.1, „Konfigurationsaufgaben“](#)
- ▶ [Abschnitt 7.2, „Erstellen einer einfachen Cluster-Konfigurationsdatei“](#)
- ▶ [Abschnitt 7.3, „Konfiguration von Fencing“](#)
- ▶ [Abschnitt 7.4, „Konfiguration von Ausfallsicherungs-Domains“](#)
- ▶ [Abschnitt 7.5, „Konfiguration von Hochverfügbarkeitsdiensten“](#)
- ▶ [Abschnitt 7.6, „Überprüfen der Konfiguration“](#)



Wichtig

Stellen Sie sicher, dass Ihr Deployment des Red Hat Hochverfügbarkeits-Add-Ons Ihren Anforderungen gerecht wird und unterstützt werden kann. Beratschlagen Sie sich dazu ggf. mit einem autorisierten Red Hat Vertreter, um Ihre Konfiguration vor dem Deployment zu verifizieren. Berücksichtigen Sie zudem eine gewisse Zeit für einen Burn-In-Test, um die Konfiguration auf mögliche Ausfälle zu überprüfen.



Wichtig

Dieses Kapitel verweist auf häufig verwendete `cluster.conf`-Elemente und -Parameter. Eine vollständige Liste samt Beschreibung aller `cluster.conf`-Elemente und -Attribute finden Sie im Cluster-Schema unter `/usr/share/cluster/cluster.rng` und dem annotierten Schema unter `/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html` (zum Beispiel `/usr/share/doc/cman-3.0.12/cluster_conf.html`).



Wichtig

Bestimmte Verfahren in diesem Kapitel erfordern, dass der `cman_tool -r`-Befehl zum Verbreiten der Cluster-Konfiguration im gesamten Cluster ausgeführt wird. Für die Verwendung dieses Befehls ist es erforderlich, dass `ricci` läuft. Die Verwendung von `ricci` erfordert ein Passwort, wenn Sie zum ersten Mal von einem bestimmten Rechner aus mit `ricci` interagieren. Informationen über den `ricci`-Dienst finden Sie in [Abschnitt 2.11, „Überlegungen zu ricci“](#).



Anmerkung

Einige Verfahren in diesem Kapitel enthalten bestimmte Befehle für die in [Anhang D, Überblick über Befehlszeilen-Tools](#) aufgelisteten Befehlszeilen-Tools. Werfen Sie für weitere Informationen über alle Befehle und Variablen einen Blick auf die Handbuchseite des jeweiligen Befehlszeilen-Tools.

7.1. Konfigurationsaufgaben

Zur Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software mit Befehlszeilen-Tools gehören die folgenden Schritte:

1. Erstellen eines Clusters. Siehe [Abschnitt 7.2, „Erstellen einer einfachen Cluster-Konfigurationsdatei“](#).
2. Konfiguration des Fencing. Siehe [Abschnitt 7.3, „Konfiguration von Fencing“](#).
3. Konfiguration von Ausfallsicherungs-Domains. Siehe [Abschnitt 7.4, „Konfiguration von Ausfallsicherungs-Domains“](#).
4. Konfiguration von Hochverfügbarkeitsdiensten. Siehe [Abschnitt 7.5, „Konfiguration von Hochverfügbarkeitsdiensten“](#).
5. Überprüfen der Konfiguration. Siehe [Abschnitt 7.6, „Überprüfen der Konfiguration“](#).

7.2. Erstellen einer einfachen Cluster-Konfigurationsdatei

Sofern die Cluster-Hardware, Red Hat Enterprise Linux und die Hochverfügbarkeits-Add-On-Software installiert sind, können Sie eine Cluster-Konfigurationsdatei (`/etc/cluster/cluster.conf`) erstellen und das Hochverfügbarkeits-Add-On starten. Dieser Abschnitt soll Ihnen als Ausgangspunkt dienen und beschreibt, wie Sie das Gerüst für eine Cluster-Konfigurationsdatei erstellen, jedoch noch ohne Fencing, Ausfallsicherungs-Domains oder Hochverfügbarkeitsdiensten - mit diesen Aspekten der Konfigurationsdatei befassen sich spätere Abschnitte.



Wichtig

Hierbei handelt es sich lediglich um einen Zwischenschritt zur Erstellung einer Cluster-Konfigurationsdatei; die hieraus resultierende Datei beinhaltet kein Fencing und ist keine gültige Konfiguration.

Die folgenden Schritte beschreiben die Erstellung und Konfiguration eines Gerüsts für eine Cluster-Konfigurationsdatei. Letztendlich unterscheidet sich die Konfigurationsdatei für Ihren Cluster abhängig von der Anzahl der Knoten, vom Fencing-Typ, von der Anzahl und der Art der Hochverfügbarkeitsdienste sowie von weiteren umgebungsspezifischen Anforderungen.

1. Erstellen Sie auf jedem Knoten im Cluster eine `/etc/cluster/cluster.conf`-Datei. Verwenden Sie dazu die Vorlage in [Beispiel 7.1, „cluster.conf-Beispiel: Grundlegende Konfiguration“](#).
2. **(Optional)** Falls Sie einen Zwei-Knoten-Cluster ausführen, können Sie die folgende Zeile zur Konfigurationsdatei hinzufügen, damit es einem einzelnen Knoten möglich ist, das Quorum zu erhalten (z.B. falls der andere Knoten ausfällt):

```
<cman two_node="1" expected_votes="1"/>
```

 Siehe [Beispiel 7.2, „cluster.conf-Beispiel: Einfache Zwei-Knoten-Konfiguration“](#).
3. Geben Sie den Cluster-Namen und die Versionsnummer der Konfiguration mithilfe dieser `cluster`-Parameter an: `name` und `config_version` (siehe [Beispiel 7.1, „cluster.conf-Beispiel: Grundlegende Konfiguration“](#) oder [Beispiel 7.2, „cluster.conf-Beispiel: Einfache Zwei-Knoten-Konfiguration“](#)).

4. Geben Sie im **clusternodes**-Abschnitt den Knotennamen und die Knoten-ID eines jeden Knotens mithilfe dieser **clusternode**-Parameter an: **name** und **nodeid**.
5. Speichern Sie die **/etc/cluster/cluster.conf** ab.
6. Überprüfen Sie die Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate**-Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Übertragen Sie die Konfigurationsdatei nach **/etc/cluster/** in jedem Cluster-Knoten. Beispielsweise könnten Sie die Datei mithilfe des **scp**-Befehls an andere Cluster-Knoten übertragen.



Anmerkung

Eine solche Übertragung der Cluster-Konfigurationsdatei ist nur beim erstmaligen Erstellen des Clusters notwendig. Sobald ein Cluster installiert wurde und läuft, kann die Cluster-Konfigurationsdatei mittels **cman_tool version -r** übertragen werden. Es ist möglich, den **scp**-Befehl zur Weitergabe einer aktualisierten Konfigurationsdatei zu verwenden, allerdings muss zur Verwendung des **scp**-Befehls auf allen Knoten die Cluster-Software gestoppt werden. Zusätzlich sollten Sie **ccs_config_validate** ausführen, falls Sie eine aktualisierte Konfigurationsdatei mittels **scp** übertragen.



Anmerkung

Es sind zwar noch andere Elemente und Parameter in der Beispielkonfigurationsdatei enthalten (z.B. **fence** und **fencedevices**), vorerst ist es jedoch nicht nötig, diese mit Informationen zu befüllen. An späterer Stelle in diesem Kapitel werden Verfahren erläutert, die Informationen zu diesen Elementen und Parametern liefern.

8. Starten Sie den Cluster. Führen Sie dazu auf jedem Cluster-Knoten den folgenden Befehl aus: **service cman start**

Zum Beispiel:

```
[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. Führen Sie auf einem beliebigen Cluster-Knoten **cman_tools nodes** aus um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[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. Läuft der Cluster, fahren Sie mit [Abschnitt 7.3, „Konfiguration von Fencing“](#) fort.

Einfache Konfigurationsbeispiele

[Beispiel 7.1, „cluster.conf-Beispiel: Grundlegende Konfiguration“](#) und [Beispiel 7.2, „cluster.conf-Beispiel: Einfache Zwei-Knoten-Konfiguration“](#) (bei einem Zwei-Knoten-Cluster) liefern jeweils eine sehr einfache Beispiel-Cluster-Konfigurationsdatei als Ausgangspunkt. An späterer Stelle in diesem Kapitel werden Verfahren erläutert, die Informationen über die Konfiguration von Fencing und Hochverfügbarkeitsdiensten liefern.

Beispiel 7.1. cluster.conf-Beispiel: Grundlegende Konfiguration

```
<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>
```

Beispiel 7.2. cluster.conf-Beispiel: Einfache Zwei-Knoten-Konfiguration

```
<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>
```

Der consensus-Wert für totem in einen Zwei-Knoten-Cluster

Wenn Sie einen Zwei-Knoten-Cluster erstellen und nicht beabsichtigen, diesem zu einem späteren Zeitpunkt weitere Knoten hinzuzufügen, dann sollten Sie den **consensus**-Wert im **totem**-Tag in der **cluster.conf**-Datei weglassen, so dass der **consensus**-Wert automatisch ermittelt wird. Beim automatischen Ermitteln des **consensus**-Werts gelten die folgenden Regeln:

- Bei zwei oder weniger Knoten lautet der **consensus**-Wert ($\text{Token} * 0.2$), mit einer Höchstgrenze von 2000 ms und einer Mindestgrenze von 200 ms.
- Bei drei oder mehr Knoten lautet der **consensus**-Wert ($\text{Token} + 2000 \text{ ms}$)

Wenn Sie das **cman**-Dienstprogramm Ihren consensus-Timeout auf diese Weise bestimmen lassen, müssen Sie später, falls Sie von zwei auf drei oder mehr Knoten aufstocken, Ihren Cluster neu starten, da der consensus-Timeout dann auf den höheren Wert geändert werden muss, entsprechend dem Token-Timeout.

Wenn Sie einen Zwei-Knoten-Cluster konfigurieren und beabsichtigen, diesen zukünftig auf mehr als zwei Knoten zu erweitern, können Sie den Consensus-Timeout außer Kraft setzen, so dass ein Cluster-Neustart nicht nötig ist, wenn Sie von zwei auf drei oder mehr Knoten aufstocken. Bearbeiten Sie dazu die **cluster.conf** wie folgt:

```
<totem token="X" consensus="X + 2000" />
```

Beachten Sie, dass bei der Analyse der Konfiguration $X + 2000$ nicht automatisch berechnet wird. Sie müssen daher einen ganzzahligen Wert einsetzen, keine Formel.

Der Vorteil bei der Verwendung des optimierten consensus-Timeouts für Zwei-Knoten-Cluster besteht darin, dass die Zeit beim Knotenwechsel im Fehlerfall reduziert wird, da consensus keine Funktion des Token-Timeouts ist.

Beachten Sie, dass für die automatische Zwei-Knoten-Erkennung in **cman** die Anzahl der physischen Knoten maßgeblich ist, nicht das Vorhandensein der **two_node=1** Direktive in der **cluster.conf**-Datei.

7.3. Konfiguration von Fencing

Zur Konfiguration von Fencing gehört (a) das Angeben eines oder mehrerer Fencing-Geräte in einem Cluster und (b) das Angeben einer oder mehrerer Fencing-Methoden für jeden Knoten (unter Verwendung der angegebenen Fencing-Geräte).

Konfigurieren Sie abhängig von dem Fencing-Gerätetyp und den Fencing-Methoden, die für Ihre Konfiguration notwendig sind, die **cluster.conf** folgendermaßen:

1. Geben Sie im **fencedevices**-Abschnitt jedes Fencing-Gerät mittels eines **fencedevice**-Elements und den vom Fencing-Gerät abhängigen Parametern an. [Beispiel 7.3, „APC Fencing-Gerät zu cluster.conf hinzugefügt“](#) zeigt ein Beispiel für eine Konfigurationsdatei, zu der ein APC-Fencing-Gerät hinzugefügt wurde.
2. Geben Sie im **clusternodes**-Abschnitt innerhalb des **fence**-Elements für jeden **clusternode**-Abschnitt die Fencing-Methode für den Knoten an. Spezifizieren Sie den Fencing-Methodenname mithilfe des **method**-Parameters **name**. Geben Sie mit dem **device**-Element und dessen Attributen **name** sowie Fencing-Gerät-spezifischer Parameter für jede Fencing-Methode das Fencing-Gerät an. [Beispiel 7.4, „Fencing-Methoden zu cluster.conf hinzugefügt“](#) zeigt ein Beispiel für eine Fencing-Methode mit einem Fencing-Gerät für jeden Knoten im Cluster.
3. Fügen Sie für andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing) im **clusternodes**-Abschnitt einen **unfence**-Abschnitt ein. Dadurch wird sichergestellt, dass ein abgegrenzter Knoten erst wieder wieder aktiviert wird, nachdem er neu gestartet wurde. Weitere Informationen über das Aufheben der Knotenabgrenzung finden Sie auf der **fence_node(8)** Handbuchseite.

Der **unfence**-Abschnitt enthält im Gegensatz zum **fence**-Abschnitt keine **method**-Abschnitte.

Er enthält direkte **device**-Referenzen, welche die entsprechenden Geräteabschnitte für **fence** widerspiegeln, sowie zusätzlich die explizite Aktion (**action**) "on" oder "enable". Dasselbe **fencedevice** wird sowohl von den **fence** als auch von **unfence device** Zeilen referenziert, und es sollten dieselben Parameter für den Knoten wiederholt werden.

Indem Sie den **action**-Parameter auf "on" oder "enable" setzen, wird dieser Knoten nach einem Neustart aktiviert. [Beispiel 7.4, „Fencing-Methoden zu `cluster.conf` hinzugefügt“](#) und [Beispiel 7.5, „`cluster.conf`: Mehrere Fencing-Methoden pro Knoten“](#) enthalten Beispiele für die **unfence**-Elemente und Parameter.

Werfen Sie für weitere Informationen über **unfence** einen Blick auf die **fence_node**-Handbuchseite.

4. Aktualisieren Sie den **config_version**-Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
5. Speichern Sie die `/etc/cluster/cluster.conf` ab.
6. **(Optional)** Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate**-Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Führen Sie den **cman_tool version -r** Befehl aus, um die Konfiguration an die übrigen Cluster-Knoten zu verbreiten. Dadurch wird auch eine zusätzliche Validierung ausgeführt. Es ist notwendig, dass **ricci** auf jedem Cluster-Knoten ausgeführt wird, um die aktualisierten Cluster-Konfigurationsinformationen verbreiten zu können.
8. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
9. Fahren Sie mit [Abschnitt 7.4, „Konfiguration von Ausfallsicherungs-Domains“](#) fort.

Falls nötig, können Sie komplexe Konfigurationen mit mehreren Fencing-Methoden pro Knoten und mit mehreren Fencing-Geräten pro Methode konfigurieren. Falls mehrere Fencing-Methoden pro Knoten konfiguriert sind und das Fencing mit der ersten Methode fehlschlägt, versucht der Fencing-Daemon **fenced** die nächste Methode usw., bis er schließlich eine Methode findet, die funktioniert.

Manchmal ist es zur Abgrenzung eines Knotens nötig, zwei I/O-Pfade oder zwei Stromversorgungen zu deaktivieren. Sie erreichen dies durch Angabe von zwei (oder mehr) Geräten innerhalb der Fencing-Methode. **fenced** führt den Fencing-Agent einmal für jede Fencing-Gerätezeile aus; alle müssen erfolgreich verlaufen, damit das Fencing insgesamt erfolgreich ist.

Komplexere Konfigurationen werden im nachfolgenden Abschnitt [„Fencing-Konfigurationsbeispiele“](#) veranschaulicht.

Weitere Informationen über die Konfiguration bestimmter Fencing-Geräte finden Sie auf der Handbuchseite eines Fencing-Gerät-Agents (z.B. auf der Handbuchseite für **fence_apc**). Des Weiteren finden Sie Informationen über Fencing-Parameter in [Anhang A, Parameter der Fencing-Geräte](#), den Fencing-Agents in `/usr/sbin/`, dem Cluster-Schema unter `/usr/share/cluster/cluster.rng`, und dem annotierten Schema unter `/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html` (z.B. `/usr/share/doc/cman-3.0.12/cluster_conf.html`).

Fencing-Konfigurationsbeispiele

Das folgende Beispiel zeigt eine einfache Konfiguration mit einer Fencing-Methode pro Knoten und einem Fencing-Gerät pro Fencing-Methode:

- ▶ [Beispiel 7.3, „APC Fencing-Gerät zu `cluster.conf` hinzugefügt“](#)
- ▶ [Beispiel 7.4, „Fencing-Methoden zu `cluster.conf` hinzugefügt“](#)

Die folgenden Beispiele zeigen komplexere Konfigurationen:

- ▶ [Beispiel 7.5, „`cluster.conf`: Mehrere Fencing-Methoden pro Knoten“](#)
- ▶ [Beispiel 7.6, „`cluster.conf`: Fencing, Mehrere Multipath-Ports“](#)

► [Beispiel 7.7, „cluster.conf: Fencing von Knoten mit Dual-Stromversorgung“](#)



Anmerkung

Die Beispiele in diesem Abschnitt können nicht alle möglichen Fälle aufzeigen, es gibt also durchaus andere Wege, wie Sie das Fencing Ihren Anforderungen entsprechend konfigurieren können.

Beispiel 7.3. APC Fencing-Gerät zu cluster.conf hinzugefügt

```
<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 diesem Beispiel wurde ein Fencing-Gerät (**fencedevice**) zum **fencedevices**-Element hinzugefügt und spezifiziert den Fencing-Agent (**agent**) als **fence_apc**, die IP-Adresse (**ipaddr**) als **apc_ip_example**, das Login (**login**) als **login_example**, den Namen des Fencing-Geräts (**name**) als **apc** und das Passwort (**passwd**) als **password_example**.

Beispiel 7.4. Fencing-Methoden zu `cluster.conf` hinzugefügt

```
<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 diesem Beispiel wurde eine Fencing-Methode (**method**) zu jedem Knoten hinzugefügt. Der Name der Fencing-Methode (**name**) für jeden Knoten ist **APC**. Das Gerät (**device**) für die Fencing-Methode in jedem Knoten spezifiziert den Namen (**name**) als **apc** und eine eindeutige APC-Schalter Netzanschlussnummer (**port**) für jeden Knoten. Zum Beispiel lautet die Anschlussnummer für `node-01.example.com` **1** (**port="1"**). Der Gerätenamen für jeden Knoten (**device name="apc"**) verweist auf das Fencing-Gerät anhand des Namens (**name**) **apc** in dieser Zeile des **fencedevices**-Elements: **fencedevice agent="fence_apc" ipaddr="apc_ip_example" login="login_example" name="apc" passwd="password_example"/**.

Beispiel 7.5. cluster.conf: Mehrere Fencing-Methoden pro Knoten

```
<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>
```

Beispiel 7.6. cluster.conf: Fencing, Mehrere Multipath-Ports

```
<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>
```


Beispiel 7.7. cluster.conf: Fencing von Knoten mit Dual-Stromversorgung

```

<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>

```

Werden Netzschalter zum Abgrenzen von Knoten mit dualer Stromversorgung verwendet, muss den Agents mitgeteilt werden, beide Netzanschlüsse zu deaktivieren, bevor die Stromversorgung auf einem der beiden Anschlüsse wiederhergestellt werden kann. Das standardmäßige Verhalten des Agents beim An- und Ausschalten könnte andernfalls dazu führen, dass die Stromversorgung auf dem Knoten nie vollständig abgeschaltet wird.

7.4. Konfiguration von Ausfallsicherungs-Domains

Eine Ausfallsicherungs-Domain ist eine benannte Teilmenge von Cluster-Knoten, die dazu berechtigt ist, einen Cluster-Dienst im Falle eines Knotenausfalls weiterzuführen. Eine Ausfallsicherungs-Domain kann die folgenden Charakteristiken haben:

- Uneingeschränkt — Ermöglicht Ihnen, eine Teilmenge bevorzugter Mitglieder zu spezifizieren, doch

der dieser Domain zugewiesene Cluster-Dienst kann auf jedem verfügbaren Mitglied ausgeführt werden.

- ▶ **Eingeschränkt** — Ermöglicht Ihnen, die Mitglieder einzuschränken, auf denen ein bestimmter Cluster-Dienst laufen darf. Falls keines der Mitglieder in einer eingeschränkten Ausfallsicherungs-Domain verfügbar ist, kann der Cluster-Dienst nicht gestartet werden (weder manuell noch durch die Cluster-Software).
- ▶ **Ungeordnet** — Wenn ein Cluster-Dienst einer ungeordneten Ausfallsicherungs-Domain zugewiesen ist, wird das Mitglied, auf dem der Cluster-Dienst ausgeführt wird, ohne Berücksichtigung von Prioritäten aus den verfügbaren Mitgliedern der Ausfallsicherungs-Domain ausgewählt.
- ▶ **Geordnet** — Ermöglicht Ihnen, eine Prioritätsreihenfolge für die Mitglieder einer Ausfallsicherungs-Domain anzugeben. Geordnete Ausfallsicherungs-Domains wählen den Knoten mit der niedrigsten Priorität zuerst. Das heißt, dass der Knoten in der Ausfallsicherungs-Domain mit der Priorität "1" die höchste Priorität hat und demnach der bevorzugte Knoten in einer Ausfallsicherungs-Domain ist. Der nächste bevorzugte Knoten wäre also der Knoten mit der nächsthöheren Priorität, usw.
- ▶ **Failback** — Ermöglicht Ihnen festzulegen, ob ein Dienst in der Ausfallsicherungs-Domain auf den Knoten zurück wechseln soll, auf dem er vor dessen Ausfall ursprünglich ausgeführt wurde. Das Konfigurieren dieser Charakteristik ist hilfreich in Situationen, in denen ein Knoten häufig ausfällt und Teil einer geordneten Ausfallsicherungs-Domain ist. In diesem Fall würde ein Dienst, der auf dem bevorzugten Knoten in einer Ausfallsicherungs-Domain läuft, möglicherweise wiederholt zwischen dem bevorzugten Knoten und einem anderen Knoten hin- und her wechseln, was beträchtliche Leistungseinbußen zur Folge hätte.



Anmerkung

Die Failback-Charakteristik greift nur, wenn die geordnete Ausfallsicherung konfiguriert ist.



Anmerkung

Eine Änderung der Ausfallsicherungs-Domain-Konfiguration hat keine Auswirkungen auf derzeit laufende Dienste.



Anmerkung

Ausfallsicherungs-Domains werden für den Betrieb *nicht* benötigt.

Standardmäßig sind Ausfallsicherungs-Domains uneingeschränkt und ungeordnet.

In einem Cluster mit mehreren Mitgliedern kann der Einsatz einer beschränkten Ausfallsicherungs-Domain Ihnen die Arbeit erleichtern. Denn um einen Cluster zum Ausführen eines Cluster-Dienstes (wie z.B. **httpd**) einzurichten, müssten Sie auf allen Cluster-Mitgliedern, die diesen Cluster-Dienst ausführen sollen, eine identische Konfiguration einrichten. Anstatt den gesamten Cluster zur Ausführung dieses Cluster-Dienstes einzurichten, müssen Sie somit nur die Mitglieder der beschränkten Ausfallsicherungs-Domain, die Sie mit diesem Cluster-Dienst verknüpfen möchten, entsprechend einrichten.



Anmerkung

Um ein bevorzugtes Mitglied zu konfigurieren, können Sie eine uneingeschränkte Ausfallsicherungs-Domain einrichten, die nur aus einem Cluster-Mitglied besteht. Dadurch läuft der Cluster-Dienst zwar hauptsächlich auf diesem einen Cluster-Mitglied (dem bevorzugten Mitglied), doch erlaubt es dem Cluster-Dienst gleichzeitig, im Falle eines Ausfalls auf einen beliebigen anderen Knoten zu wechseln.

Gehen Sie folgendermaßen vor, um eine Ausfallsicherungs-Domain zu konfigurieren:

1. Öffnen Sie `/etc/cluster/cluster.conf` auf einem beliebigen Knoten im Cluster.
2. Fügen Sie das folgende Gerüst innerhalb des `rm`-Elements für jede zu verwendende Ausfallsicherungs-Domain ein:

```
<failoverdomains>
  <failoverdomain name="" nofailback="" ordered="" restricted="">
    <failoverdomainnode name="" priority=""/>
    <failoverdomainnode name="" priority=""/>
    <failoverdomainnode name="" priority=""/>
  </failoverdomain>
</failoverdomains>
```



Anmerkung

Die Anzahl der `failoverdomainnode`-Parameter hängt von der Anzahl der Knoten in der Ausfallsicherungs-Domain ab. Das oben gezeigte Gerüst für den `failoverdomain`-Abschnitt enthält drei `failoverdomainnode`-Elemente (ohne spezifizierte Knotennamen), was bedeutet, dass es drei Knoten in der Ausfallsicherungs-Domain gibt.

3. Geben Sie im `failoverdomain`-Abschnitt die Werte für die Elemente und Parameter an. Beschreibungen der Elemente und Parameter finden Sie im `failoverdomain`-Abschnitt des annotierten Cluster-Schemas. Das annotierte Cluster-Schema ist in jedem Cluster-Knoten verfügbar unter `/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html` (z.B. `/usr/share/doc/cman-3.0.12/cluster_conf.html`). Ein Beispiel für einen `failoverdomains`-Abschnitt finden Sie in [Beispiel 7.8, „Eine Ausfallsicherungs-Domain zu cluster.conf hinzugefügt“](#).
4. Aktualisieren Sie den `config_version`-Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von `config_version="2"` auf `config_version="3"`).
5. Speichern Sie die `/etc/cluster/cluster.conf` ab.
6. **(Optional)** Überprüfen Sie die Datei anhand des Cluster-Schemas (`cluster.rng`), indem Sie den `ccs_config_validate`-Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Führen Sie den Befehl `cman_tool version -r` aus, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
8. Fahren Sie mit [Abschnitt 7.5, „Konfiguration von Hochverfügbarkeitsdiensten“](#) fort.

[Beispiel 7.8, „Eine Ausfallsicherungs-Domain zu cluster.conf hinzugefügt“](#) zeigt ein Beispiel für eine Konfiguration mit einer geordneten, uneingeschränkten Ausfallsicherungs-Domain.

Beispiel 7.8. Eine Ausfallsicherungs-Domain zu `cluster.conf` hinzugefügt

```

<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>

```

Der **failoverdomains**-Abschnitt enthält einen **failoverdomain**-Abschnitt für jede Ausfallsicherungs-Domain im Cluster. Dieses Beispiel hat eine Ausfallsicherungs-Domain. In der **failoverdomain**-Zeile ist der Name (**name**) als **example_pri** spezifiziert. Zusätzlich wird kein Failback (**failback="0"**), eine geordnete Ausfallsicherung (**ordered="1"**) und die Ausfallsicherungs-Domain als uneingeschränkt (**restricted="0"**) spezifiziert.

7.5. Konfiguration von Hochverfügbarkeitsdiensten

Die Konfiguration von Hochverfügbarkeitsdiensten umfasst das Konfigurieren von Ressourcen und das Zuweisen derselben zu Diensten.

Die folgenden Abschnitte beschreiben, wie Sie **/etc/cluster/cluster.conf** zum Hinzufügen von Ressourcen und Diensten konfigurieren.

- ▶ [Abschnitt 7.5.1, „Hinzufügen von Cluster-Ressourcen“](#)
- ▶ [Abschnitt 7.5.2, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#)



Wichtig

Es gibt eine Vielzahl möglicher Konfigurationen für die Hochverfügbarkeitsressourcen und -dienste. Für ein besseres Verständnis von Ressourcenparametern und Ressourcenverhalten werfen Sie einen Blick auf [Anhang B, Parameter der Hochverfügbarkeitsressourcen](#) and [Anhang C, Verhalten der Hochverfügbarkeitsressourcen](#). Um optimale Leistung zu erreichen und um sicherzustellen, dass Ihre Konfiguration unterstützt werden kann, setzen Sie sich bitte mit einem autorisierten Red Hat Vertreter in Verbindung.

7.5.1. Hinzufügen von Cluster-Ressourcen

Sie können zwei Arten von Ressourcen konfigurieren:

- ▶ Global — Ressourcen, die für jeden Dienst im Cluster zur Verfügung stehen. Diese werden im **resources**-Abschnitt der Konfigurationsdatei konfiguriert (innerhalb des **rm**-Elements).
- ▶ Dienst-spezifisch — Ressourcen, die nur für einen einzigen Dienst zur Verfügung stehen. Diese werden im jeweiligen **service**-Abschnitt der Konfigurationsdatei konfiguriert (innerhalb des **rm**-Elements).

Dieser Abschnitt beschreibt, wie globale Ressourcen hinzugefügt werden. Verfahren zum Konfigurieren von dienstspezifischen Ressourcen finden Sie in [Abschnitt 7.5.2, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#).

Um eine globale Cluster-Ressource hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Öffnen Sie `/etc/cluster/cluster.conf` auf einem beliebigen Knoten im Cluster.
2. Fügen Sie einen **resources**-Abschnitt innerhalb des **rm**-Elements hinzu. Zum Beispiel:

```
<rm>
  <resources>

  </resources>
</rm>
```

3. Befüllen Sie es abhängig von den Diensten, die Sie erstellen möchten, mit Ressourcen. Sehen Sie nachfolgend beispielsweise die Ressourcen, die in einem Apache-Dienst verwendet werden. Dazu gehören eine Dateisystemressource (**fs**), eine IP-Ressource (**ip**) und eine Apache-Ressource (**apache**).

```
<rm>
  <resources>
    <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
    <ip address="127.143.131.100" monitor_link="on" sleeptime="10"/>
    <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
  </resources>
</rm>
```

[Beispiel 7.9, „cluster.conf-Datei mit hinzugefügten Ressourcen“](#) zeigt ein Beispiel einer `cluster.conf`-Datei mit hinzugefügtem **resources**-Abschnitt.

4. Aktualisieren Sie den **config_version**-Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
5. Speichern Sie die `/etc/cluster/cluster.conf` ab.
6. **(Optional)** Überprüfen Sie die Datei anhand des Cluster-Schemas (`cluster.rng`), indem Sie

den `ccs_config_validate`-Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Führen Sie den Befehl `cman_tool version -r` aus, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
8. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
9. Fahren Sie mit [Abschnitt 7.5.2, „Hinzufügen eines Cluster-Dienstes zum Cluster“](#) fort.

Beispiel 7.9. `cluster.conf`-Datei mit hinzugefügten Ressourcen

```
<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="on" sleeptime="10"/>
      <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
    </resources>
  </rm>
</cluster>
```

7.5.2. Hinzufügen eines Cluster-Dienstes zum Cluster

Um einen Cluster-Dienst zum Cluster hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Öffnen Sie `/etc/cluster/cluster.conf` auf einem beliebigen Knoten im Cluster.
2. Fügen Sie für jeden Dienst einen **service**-Abschnitt innerhalb des **rm**-Elements hinzu. Zum Beispiel:

```
<rm>
  <service autostart="1" domain="" exclusive="0" name=""
  recovery="restart">

  </service>
</rm>
```

3. Konfigurieren Sie die folgenden Parameter im **service**-Element:
 - ▶ **autostart** — Legt fest, ob der Dienst beim Start des Clusters automatisch gestartet werden soll.
 - ▶ **domain** — Legt eine Ausfallsicherungs-Domain fest (falls erforderlich).
 - ▶ **exclusive** — Legt eine Richtlinie fest, gemäß der dieser Dienst ausschließlich auf Knoten ausgeführt werden darf, auf denen kein anderer Dienst läuft.
 - ▶ **recovery** — Legt eine Richtlinie zur Wiederherstellung des Dienstes fest. Zu den Optionen gehören der Neustart, die Verlegung oder die Deaktivierung des Dienstes.
4. Abhängig von der Art der Ressource, die Sie verwenden möchten, befüllen Sie den Dienst mit globalen oder dienstspezifischen Ressourcen.

Sehen Sie hier beispielsweise einen Apache-Dienst, der globale Ressourcen verwendet:

```
<rm>
  <resources>
    <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
    fstype="ext3"/>
    <ip address="127.143.131.100" monitor_link="on"
    sleeptime="10"/>
    <apache config_file="conf/httpd.conf" name="example_server"
    server_root="/etc/httpd" shutdown_wait="0"/>
  </resources>
  <service autostart="1" domain="example_pri" exclusive="0"
  name="example_apache" recovery="relocate">
    <fs ref="web_fs"/>
    <ip ref="127.143.131.100"/>
    <apache ref="example_server"/>
  </service>
</rm>
```

Und sehen Sie hier beispielsweise einen Apache-Dienst, der dienstspezifische Ressourcen verwendet:


```
<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="on"
sleeptime="10"/>
    <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
  </service>
</rm>
```

[Beispiel 7.10, „cluster.conf mit hinzugefügten Diensten: Einer verwendet globale Ressourcen, der andere verwendet dienstspezifische Ressourcen“](#) zeigt ein Beispiel einer `cluster.conf`-Datei mit zwei Diensten:

- ▶ **example_apache** — Dieser Dienst verwendet die globalen Ressourcen `web_fs`, `127.143.131.100` und `example_server`.
- ▶ **example_apache2** — Dieser Dienst verwendet die dienstspezifischen Ressourcen `web_fs2`, `127.143.131.101` und `example_server2`.

5. Aktualisieren Sie den `config_version`-Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von `config_version="2"` auf `config_version="3"`).
6. Speichern Sie die `/etc/cluster/cluster.conf` ab.
7. **(Optional)** Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (`cluster.rng`), indem Sie den `ccs_config_validate`-Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

8. Führen Sie den Befehl `cman_tool version -r` aus, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
9. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
10. Fahren Sie mit [Abschnitt 7.6, „Überprüfen der Konfiguration“](#) fort.

Beispiel 7.10. cluster.conf mit hinzugefügten Diensten: Einer verwendet globale Ressourcen, der andere verwendet dienstspezifische Ressourcen

```

<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="on" sleeptime="10"/>
      <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
    </resources>
    <service autostart="1" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
      <fs ref="web_fs"/>
      <ip ref="127.143.131.100"/>
      <apache ref="example_server"/>
    </service>
    <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="on" sleeptime="10"/>
      <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
    </service>
  </rm>
</cluster>

```

7.6. Überprüfen der Konfiguration

Nachdem Sie Ihre Cluster-Konfigurationsdatei erstellt haben, überprüfen Sie, ob diese einwandfrei funktioniert, indem Sie die folgenden Schritte ausführen:

1. Führen Sie auf jedem Knoten einen Neustart der Cluster-Software aus. Dadurch wird sichergestellt, dass auch solche Konfigurationsänderungen, die nur beim Start überprüft werden, für die aktuelle Konfiguration berücksichtigt werden. Sie können die Cluster-Software durch Ausführen von **service cman restart** neu starten. Zum Beispiel:

```
[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. Führen Sie **service clvmd start** aus, falls CLVM zum Erstellen geclusterter Datenträger verwendet wird. Zum Beispiel:

```
[root@example-01 ~]# service clvmd start
Activating VGs:                    [ OK ]
```

3. Führen Sie **service gfs2 start** aus, falls Sie Red Hat GFS2 verwenden. Zum Beispiel:

```
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA): [ OK ]
Mounting GFS2 filesystem (/mnt/gfsB): [ OK ]
```

4. Führen Sie **service rgmanager start** aus, falls Sie Hochverfügbarkeitsdienste verwenden. Zum Beispiel:

```
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:  [ OK ]
```

5. Führen Sie auf einem beliebigen Cluster-Knoten **cman_tool nodes** aus um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[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. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **clustat**-Dienstprogramms, ob die Hochverfügbarkeitsdienste wie erwartet funktionieren. Zusätzlich zeigt **clustat** den Status der Cluster-Knoten. Zum Beispiel:

```
[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. Wenn der Cluster wie erwartet funktioniert, sind Sie mit dem Erstellen der Konfigurationsdatei fertig. Sie können den Cluster mit den in [Kapitel 8, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#) beschriebenen Befehlszeilen-Tools verwalten.

Kapitel 8. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools

Dieses Kapitel erläutert die verschiedenen administrativen Aufgaben zur Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons und umfasst die folgenden Abschnitte:

- ▶ [Abschnitt 8.1, „Starten und Stoppen der Cluster-Software“](#)
- ▶ [Abschnitt 8.2, „Hinzufügen oder Löschen eines Knotens“](#)
- ▶ [Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“](#)
- ▶ [Abschnitt 8.4, „Aktualisieren einer Konfiguration“](#)



Wichtig

Stellen Sie sicher, dass Ihr Deployment des Red Hat Hochverfügbarkeits-Add-Ons Ihren Anforderungen gerecht wird und unterstützt werden kann. Beratschlagen Sie sich dazu ggf. mit einem autorisierten Red Hat Vertreter, um Ihre Konfiguration vor dem Deployment zu verifizieren. Berücksichtigen Sie zudem eine gewisse Zeit für einen Burn-In-Test, um die Konfiguration auf mögliche Ausfälle zu überprüfen.



Wichtig

Dieses Kapitel verweist auf häufig verwendete `cluster.conf`-Elemente und -Parameter. Eine vollständige Liste samt Beschreibung aller `cluster.conf`-Elemente und -Attribute finden Sie im Cluster-Schema unter `/usr/share/cluster/cluster.rng` und dem annotierten Schema unter `/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html` (zum Beispiel `/usr/share/doc/cman-3.0.12/cluster_conf.html`).



Wichtig

Bestimmte Verfahren in diesem Kapitel erfordern, dass der `cman_tool -r`-Befehl zum Verbreiten der Cluster-Konfiguration im gesamten Cluster ausgeführt wird. Für die Verwendung dieses Befehls ist es erforderlich, dass `ricci` läuft.



Anmerkung

Einige Verfahren in diesem Kapitel enthalten bestimmte Befehle für die in [Anhang D, Überblick über Befehlszeilen-Tools](#) aufgelisteten Befehlszeilen-Tools. Werfen Sie für weitere Informationen über alle Befehle und Variablen einen Blick auf die Handbuchseite des jeweiligen Befehlszeilen-Tools.

8.1. Starten und Stoppen der Cluster-Software

Sie können die Cluster-Software auf einem Knoten gemäß [Abschnitt 8.1.1, „Starten der Cluster-Software“](#) und [Abschnitt 8.1.2, „Stoppen der Cluster-Software“](#) starten und stoppen. Das Starten der Cluster-Software auf einem Knoten veranlasst diesen dazu, dem Cluster beizutreten; das Stoppen der Cluster-Software auf einem Knoten veranlasst ihn dazu, den Cluster zu verlassen.

8.1.1. Starten der Cluster-Software

Um die Cluster-Software auf einem Knoten zu starten, führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

1. **service cman start**
2. **service clvmd start**, falls CLVM zum Erstellen geclusterter Datenträger verwendet wird
3. **service gfs2 start**, falls Sie Red Hat GFS2 verwenden
4. **service rgmanager start**, falls Sie Hochverfügbarkeitsdienste verwenden (**rgmanager**)

Zum Beispiel:

```
[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. Stoppen der Cluster-Software

Um die Cluster-Software auf einem Knoten zu stoppen, führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

1. **service rgmanager stop**, falls Sie Hochverfügbarkeitsdienste verwenden (**rgmanager**)
2. **service gfs2 stop**, falls Sie Red Hat GFS2 verwenden
3. **umount -at gfs2**, falls Sie Red Hat GFS2 in Verbindung mit dem **rgmanager** verwenden, um sicherzustellen, dass jegliche GFS2-Dateien, die während des Starts von **rgmanager** eingehängt wurden (jedoch beim Beenden nicht ausgehängt wurden) ebenfalls ausgehängt werden.
4. **service clvmd stop**, falls CLVM zum Erstellen geclusterter Datenträger verwendet wird
5. **service cman stop**

Zum Beispiel:

```
[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 ~]#
```



Anmerkung

Durch das Stoppen der Cluster-Software auf einem Knoten wechseln dessen Hochverfügbarkeitsdienste auf einen anderen Knoten. Alternativ dazu können Sie in Erwägung ziehen, die Hochverfügbarkeitsdienste vor dem Stoppen der Cluster-Software auf einen anderen Knoten zu verlegen oder zu migrieren. Informationen über das Verwalten von Hochverfügbarkeitsdiensten finden Sie in [Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“](#).

8.2. Hinzufügen oder Löschen eines Knotens

Dieser Abschnitt beschreibt, wie ein Knoten von einem Cluster entfernt wird und wie ein Knoten zu einem Cluster hinzugefügt wird. Sie können einen Knoten von einem Cluster löschen gemäß [Abschnitt 8.2.1, „Einen Knoten vom Cluster löschen“](#); und Sie können einen Knoten zu einem Cluster hinzufügen gemäß [Abschnitt 8.2.2, „Einen Knoten zum Cluster hinzufügen“](#).

8.2.1. Einen Knoten vom Cluster löschen

Das Löschen eines Knotens vom Cluster umfasst das Stoppen der Cluster-Software auf dem zu löschenden Knoten und das Aktualisieren der Cluster-Konfiguration, um die Änderung widerzuspiegeln.



Wichtig

Falls der Cluster durch das Löschen eines Knotens nunmehr nur noch zwei Knoten umfasst, müssen Sie die Cluster-Software auf beiden Knoten nach Änderung der Konfigurationsdatei neu starten.

Um einen Knoten von einem Cluster zu löschen, führen Sie die folgenden Schritte aus:

1. Verwenden Sie auf einem beliebigen Knoten das **clusvcadm**-Dienstprogramm, um alle Hochverfügbarkeitsdienste, die auf dem zu löschenden Knoten laufen, entweder zu verlegen, zu migrieren oder zu stoppen. Weitere Informationen zur Verwendung von **clusvcadm** finden Sie in [Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“](#).
2. Stoppen Sie auf dem zu löschenden Knoten die Cluster-Software gemäß [Abschnitt 8.1.2, „Stoppen der Cluster-Software“](#). Zum Beispiel:


```
[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. Bearbeiten Sie auf einem beliebigen Knoten im Cluster die `/etc/cluster/cluster.conf`, um den `clusternode`-Abschnitt des zu löschenden Knotens zu entfernen. Falls z.B. `node-03.example.com` in [Beispiel 8.1, „Drei-Knoten-Cluster-Konfiguration“](#) entfernt werden soll, löschen Sie den `clusternode`-Abschnitt für diesen Knoten. Falls der Cluster durch das Löschen eines Knotens nunmehr nur noch zwei Knoten umfasst, können Sie die folgende Zeile zur Konfigurationsdatei hinzufügen, damit ein einzelner Knoten das Quorum erhalten kann (falls z.B. ein Knoten ausfällt):

```
<cman two_node="1" expected_votes="1"/>
```

Siehe [Abschnitt 8.2.3, „Beispiele für Drei-Knoten- und Zwei-Knoten-Konfigurationen“](#) für einen Vergleich einer Drei-Knoten- und einer Zwei-Knoten-Konfiguration.

4. Aktualisieren Sie den `config_version`-Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von `config_version="2"` auf `config_version="3"`).
5. Speichern Sie die `/etc/cluster/cluster.conf` ab.
6. **(Optional)** Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (`cluster.rng`), indem Sie den `ccs_config_validate`-Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Führen Sie den Befehl `cman_tool version -r` aus, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
8. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
9. Falls der Cluster durch das Löschen eines Knotens nunmehr nur noch zwei Knoten umfasst, müssen Sie die Cluster-Software wie folgt neu starten:
 - a. Stoppen Sie auf jedem Knoten die Cluster-Software gemäß [Abschnitt 8.1.2, „Stoppen der Cluster-Software“](#). Zum Beispiel:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager: [ OK ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA): [ OK ]
Unmounting GFS2 filesystem (/mnt/gfsB): [ OK ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit [ OK ]
clvmd terminated [ OK ]
[root@example-01 ~]# service cman stop
Stopping cluster:
  Leaving fence domain... [ OK ]
  Stopping gfs_controld... [ OK ]
  Stopping dlm_controld... [ OK ]
  Stopping fenced... [ OK ]
  Stopping cman... [ OK ]
  Waiting for corosync to shutdown: [ OK ]
  Unloading kernel modules... [ OK ]
  Unmounting configfs... [ OK ]
[root@example-01 ~]#
```

- b. Starten Sie auf jedem Knoten die Cluster-Software gemäß [Abschnitt 8.1.1. „Starten der Cluster-Software“](#). Zum Beispiel:

```
[root@example-01 ~]# service cman start
Starting cluster:
  Checking Network Manager... [ OK ]
  Global setup... [ OK ]
  Loading kernel modules... [ OK ]
  Mounting configfs... [ OK ]
  Starting cman... [ OK ]
  Waiting for quorum... [ OK ]
  Starting fenced... [ OK ]
  Starting dlm_controld... [ OK ]
  Starting gfs_controld... [ OK ]
  Unfencing self... [ OK ]
  Joining fence domain... [ OK ]
[root@example-01 ~]# service clvmd start
Starting clvmd: [ OK ]
Activating VG(s): 2 logical volume(s) in volume group "vg_example" now
active [ OK ]

[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA): [ OK ]
Mounting GFS2 filesystem (/mnt/gfsB): [ OK ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager: [ OK ]
[root@example-01 ~]#
```

- c. Führen Sie auf einem beliebigen Cluster-Knoten **cman_tools nodes** aus um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts  Inc  Joined  Name
  1    M   548  2010-09-28 10:52:21  node-01.example.com
  2    M   548  2010-09-28 10:52:21  node-02.example.com
```

- d. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **clustat**-Dienstprogramms, ob die Hochverfügbarkeitsdienste wie erwartet funktionieren. Zusätzlich zeigt **clustat** den Status der Cluster-Knoten. Zum Beispiel:

```
[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. Einen Knoten zum Cluster hinzufügen

Das Hinzufügen eines Knotens zum Cluster umfasst das Aktualisieren der Cluster-Konfiguration, das Übertragen der aktualisierten Konfiguration auf den hinzuzufügenden Knoten, und das Starten der Cluster-Software auf diesem Knoten. Um einen Knoten zu einem Cluster hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Bearbeiten Sie auf einem beliebigen Knoten im Cluster die `/etc/cluster/cluster.conf`-Datei, um einen `clusternode`-Abschnitt für den neuen Knoten hinzuzufügen. Um in [Beispiel 8.2, „Zwei-Knoten-Cluster-Konfiguration“](#) beispielsweise `node-03.example.com` hinzuzufügen, fügen Sie einen `clusternode`-Abschnitt für diesen Knoten ein. Falls der Cluster durch das Hinzufügen eines Knotens von vormals zwei Knoten auf nun drei oder mehr Knoten anwächst, entfernen Sie die folgenden `cman`-Parameter aus der `/etc/cluster/cluster.conf`:

- ▶ `cman two_node="1"`
- ▶ `expected_votes="1"`

Siehe [Abschnitt 8.2.3, „Beispiele für Drei-Knoten- und Zwei-Knoten-Konfigurationen“](#) für einen Vergleich einer Drei-Knoten- und einer Zwei-Knoten-Konfiguration.

2. Aktualisieren Sie den `config_version`-Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von `config_version="2"` auf `config_version="3"`).
3. Speichern Sie die `/etc/cluster/cluster.conf` ab.
4. **(Optional)** Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (`cluster.rng`), indem Sie den `ccs_config_validate`-Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

5. Führen Sie den Befehl `cman_tool version -r` aus, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
6. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
7. Übertragen Sie die aktualisierte Konfigurationsdatei nach `/etc/cluster/` in jedem Knoten, der zum Cluster hinzugefügt werden soll. Verwenden Sie beispielsweise den `scp`-Befehl, um die aktualisierte Konfigurationsdatei auf jeden hinzuzufügenden Knoten zu übertragen.
8. Falls die Anzahl der Knoten im Cluster durch das Hinzufügen von Knoten nunmehr mehr als zwei Knoten umfasst, müssen Sie die Cluster-Software in den vorhandenen Cluster-Knoten wie folgt neu starten:
 - a. Stoppen Sie auf jedem Knoten die Cluster-Software gemäß [Abschnitt 8.1.2, „Stoppen der Cluster-Software“](#). Zum Beispiel:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager: [ OK ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA): [ OK ]
Unmounting GFS2 filesystem (/mnt/gfsB): [ OK ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit [ OK ]
clvmd terminated [ OK ]
[root@example-01 ~]# service cman stop
Stopping cluster:
  Leaving fence domain... [ OK ]
  Stopping gfs_controld... [ OK ]
  Stopping dlm_controld... [ OK ]
  Stopping fenced... [ OK ]
  Stopping cman... [ OK ]
  Waiting for corosync to shutdown: [ OK ]
  Unloading kernel modules... [ OK ]
  Unmounting configfs... [ OK ]
[root@example-01 ~]#
```

- b. Starten Sie auf jedem Knoten die Cluster-Software gemäß [Abschnitt 8.1.1, „Starten der Cluster-Software“](#). Zum Beispiel:

```
[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. Starten Sie auf jedem Knoten, der zum Cluster hinzugefügt werden soll, die Cluster-Software gemäß [Abschnitt 8.1.1, „Starten der Cluster-Software“](#). Zum Beispiel:

```
[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. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **clustat**-Dienstprogramms, dass jeder hinzugefügte Knoten läuft und Teil des Clusters ist. Zum Beispiel:

```
[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
```

Informationen über die Verwendung von **clustat** finden Sie in [Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“](#).

Zusätzlich können Sie **cman_tool status** dazu verwenden, um die Knotenstimmen, Knotenanzahl und Quorum-Zahl zu überprüfen. Zum Beispiel:

```
[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. Sie können auf einem beliebigen Knoten das **cclusvcadm**-Dienstprogramm verwenden, um einen laufenden Dienst auf den neu beigetretenen Knoten zu verlegen oder zu migrieren. Sie können auch eventuell deaktivierte Dienste aktivieren. Informationen über die Verwendung von **cclusvcadm** finden Sie in [Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“](#)

8.2.3. Beispiele für Drei-Knoten- und Zwei-Knoten-Konfigurationen

Werfen Sie einen Blick auf die nachfolgenden Beispiele für einen Vergleich einer Drei-Knoten- und einer Zwei-Knoten-Konfiguration.

Beispiel 8.1. Drei-Knoten-Cluster-Konfiguration

```

<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="on" 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="on" sleeptime="10"/>
      <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
    </service>
  </rm>
</cluster>

```


Beispiel 8.2. Zwei-Knoten-Cluster-Konfiguration

```

<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>
    </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"/>
      </failoverdomain>
    </failoverdomains>
    <resources>
      <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
      <ip address="127.143.131.100" monitor_link="on" sleeptime="10"/>
      <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
    </resources>
    <service autostart="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="on" sleeptime="10"/>
      <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
    </service>
  </rm>
</cluster>

```

8.3. Verwaltung von Hochverfügbarkeitsdiensten

Sie können Hochverfügbarkeitsdienste mithilfe der **Cluster Status Utility**, `c lustat`, und der **Cluster User Service Administration Utility**, `c lusvcadm` verwalten. `c lustat` zeigt den Status eines

Clusters und **clusvcadm** ermöglicht die Verwaltung von Hochverfügbarkeitsdiensten.

Dieser Abschnitt liefert grundlegende Informationen über die Verwaltung von Hochverfügbarkeitsdiensten mithilfe von **clustat** und **clusvcadm**. Er besteht aus den folgenden Unterabschnitten:

- ▶ [Abschnitt 8.3.1, „Anzeige des Hochverfügbarkeitsdienst-Status mit clustat“](#)
- ▶ [Abschnitt 8.3.2, „Verwaltung von Hochverfügbarkeitsdiensten mit clusvcadm“](#)

8.3.1. Anzeige des Hochverfügbarkeitsdienst-Status mit clustat

clustat zeigt den clusterweiten Status an. Es zeigt Informationen über Mitgliedschaften, die Quorum-Ansicht, den Status aller Hochverfügbarkeitsdienste, und es gibt außerdem an, auf welchem Knoten der **clustat**-Befehl ausgeführt wird (lokal). [Tabelle 8.1, „Dienst-Status“](#) beschreibt die Status, in denen sich die Dienste befinden können und die durch Ausführen von **clustat** angezeigt werden. [Beispiel 8.3, „clustat-Anzeige“](#) zeigt ein Beispiel einer **clustat**-Anzeige. Detailliertere Informationen zum Ausführen des **clustat**-Befehls finden Sie auf der **clustat**-Handbuchseite.

Tabelle 8.1. Dienst-Status

| Dienst-Status | Beschreibung |
|----------------------|---|
| Started | Die Dienstressourcen sind konfiguriert und stehen dem Cluster-System, das diesen Dienst besitzt, zur Verfügung. |
| Recovering | Der Dienst wartet darauf, auf einem anderen Knoten zu starten. |
| Disabled | Der Dienst wurde deaktiviert und ist keinem Besitzer zugewiesen. Ein deaktivierter Dienst wird niemals automatisch vom Cluster neu gestartet. |
| Stopped | In gestopptem Zustand wird der Dienst für einen Start nach der nächsten Dienst- oder Knotenänderung evaluiert. Es handelt sich um einen vorübergehenden Status. Sie können den Dienst von diesem Status aus deaktivieren oder aktivieren. |
| Failed | Der Dienst ist vermutlich tot. Ein Dienst wird in diesen Status versetzt, wenn die <i>stop</i> -Operation einer Ressource fehlschlägt. Nachdem ein Dienst in diesen Status versetzt wurde, müssen Sie sicherstellen, dass keine Ressourcen (z.B. ein eingehängtes Dateisystem) zugewiesen sind, bevor Sie eine disable -Anfrage senden. Die einzige Operation, die auf einem Dienst mit diesem Status ausgeführt werden kann, ist disable . |
| Uninitialized | Dieser Status kann in bestimmten Fällen während des Starts und des Ausführens von clustat -f auftreten. |

Beispiel 8.3. clustat-Anzeige

```
[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. Verwaltung von Hochverfügbarkeitsdiensten mit clusvcadm


Sie können Hochverfügbarkeitsdienste mithilfe des **c1usvcdm**-Befehls verwalten. Damit können Sie die folgenden Operationen ausführen:

- ▶ Aktivieren und Starten eines Dienstes
- ▶ Deaktivieren eines Dienstes
- ▶ Stoppen eines Dienstes
- ▶ Einfrieren eines Dienstes
- ▶ Einfrieren eines Dienstes aufheben
- ▶ Migrieren eines Dienstes (nur für Dienste auf virtuellen Maschinen)
- ▶ Verlegen eines Dienstes
- ▶ Neustarten eines Dienstes

[Tabelle 8.2, „Dienstoperationen“](#) beschreibt die Operationen im Detail. Eine vollständige Beschreibung dessen, wie diese Operationen ausgeführt werden, finden Sie auf der Handbuchseite des **c1usvcdm**-Dienstprogramms.

Tabelle 8.2. Dienstoperationen

| Dienst-Operation | Beschreibung | Befehlssyntax |
|------------------|---|---|
| Enable | Startet den Dienst, optional auf einem bevorzugten Ziel und optional gemäß der Regeln zur Ausfallsicherungs-Domain. Wird keines der beiden angegeben, wird der Dienst auf dem lokalen Host gestartet, auf dem clusvcadm ausgeführt wird. Falls der ursprüngliche <i>start</i> fehlschlägt, verhält sich der Dienst, als ob eine <i>relocate</i> -Operation angefragt wurde (siehe Relocate in dieser Tabelle). Falls die Operation erfolgreich ist, wird der Dienst in den "Started"-Status versetzt. | clusvcadm -e <service_name> oder clusvcadm -e <service_name> -m <member> (Die -m Option gibt das bevorzugte Zielmitglied an, auf dem der Dienst gestartet werden soll.) |
| Disable | Stoppt den Dienst und versetzt ihn in den "Disabled"-Zustand. Dies ist die einzig zulässige Operation, wenn sich ein Dienst im <i>failed</i> -Status befindet. | clusvcadm -d <service_name> |
| Relocate | Verlegt den Dienst auf einen anderen Knoten. Optional können Sie einen bevorzugten Knoten angeben, auf den der Dienst verlegt werden soll. Kann der Dienst nicht auf diesem bevorzugten Knoten ausgeführt werden (z.B. weil der Start des Dienstes fehlschlägt oder der Host offline ist, so verhindert dies jedoch nicht die Verlegung, sondern es wird stattdessen ein anderer Knoten ausgewählt. rgmanager versucht, den Dienst auf jedem zulässigen Knoten im Cluster zu starten. Falls keiner der zulässigen Zielknoten im Cluster den Dienst erfolgreich starten kann, schlägt die Verlegung fehl und es wird versucht, den Dienst auf dem ursprünglichen Besitzer neu zu starten. Falls der ursprüngliche Besitzer den Dienst nicht neu starten kann, wird der Dienst in den <i>stopped</i> -Status versetzt. | clusvcadm -r <service_name> oder clusvcadm -r <service_name> -m <member> (Die -m Option gibt das bevorzugte Zielmitglied an, auf dem der Dienst gestartet werden soll.) |
| Stop | Stoppt den Dienst und versetzt ihn in den <i>stopped</i> -Status. | clusvcadm -s <service_name> |
| Freeze | Friert einen Dienst auf dem Knoten ein, auf dem er derzeit ausgeführt wird. Dies verhindert sowohl Überprüfungen des Dienststatus als auch die Ausfallsicherung, falls der Knoten ausfällt oder rgmanager gestoppt wird. Dies kann verwendet werden, um einen Dienst auszusetzen, wenn Wartungsarbeiten an den zugrunde liegenden Ressourcen nötig sind. Siehe „Überlegungen zur Verwendung der Freeze- und Unfreeze-Operationen“ für wichtige Informationen über die Verwendung der <i>freeze</i> und <i>unfreeze</i> -Operationen. | clusvcadm -Z <service_name> |
| Unfreeze | Hebt den <i>freeze</i> -Status eines Dienstes wieder auf. Dadurch werden | clusvcadm -U <service_name> |

| | | |
|----------------|---|--|
| | Überprüfungen des Status wieder ermöglicht. Siehe „Überlegungen zur Verwendung der Freeze- und Unfreeze-Operationen“ für wichtige Informationen über die Verwendung der <i>freeze</i> und <i>unfreeze</i> -Operationen. | |
| Migrate | Migriert eine virtuelle Maschine auf einen anderen Knoten. Sie müssen dabei einen Zielknoten angeben. Abhängig vom Scheitern kann ein Scheitern dieser Migration dazu führen, dass die virtuelle Maschine in den <i>failed</i> -Zustand oder den "Started"-Zustand auf dem ursprünglichen Besitzer versetzt wird. | <pre>clusvcadm -M <service_name> -m <member></pre> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Wichtig Für die <i>migrate</i>-Operation <i>müssen</i> Sie mithilfe der <code>-m <member></code>-Option einen Zielknoten spezifizieren. </div> |
| Restart | Startet einen Dienst auf dem Knoten, auf dem er derzeit ausgeführt wird, neu. | <pre>clusvcadm -R <service_name></pre> |

Überlegungen zur Verwendung der Freeze- und Unfreeze-Operationen

Die Verwendung der *freeze*-Operation erlaubt die Wartung von Teilen des **rgmanager**-Dienstes. Falls Sie beispielsweise eine Datenbank und einen Webserver in einem **rgmanager**-Dienst haben, können Sie den **rgmanager**-Dienst einfrieren, die Datenbank stoppen, die Wartungsarbeiten durchführen, die Datenbank neu starten, und das Einfrieren des Dienstes anschließend wieder aufheben.

Wenn ein Dienst eingefroren ist, verhält er sich folgendermaßen:

- ▶ *Status*-Überprüfungen sind deaktiviert.
- ▶ *Start*-Operationen sind deaktiviert.
- ▶ *Stop*-Operationen sind deaktiviert.
- ▶ Es erfolgt keine Ausfallsicherung (selbst wenn Sie den Besitzer des Dienstes abschalten).



Wichtig

Werden die folgenden Richtlinien nicht befolgt, kann das ggf. dazu führen, dass Ressourcen mehreren Hosts zugewiesen werden:

- ▶ Sie *dürfen nicht* alle Instanzen des **rgmanager** stoppen, wenn ein Dienst eingefroren ist, es sei denn, Sie planen vor dem Neustart von **rgmanager** einen Neustart der Hosts.
- ▶ Sie *dürfen nicht* das Einfrieren eines Dienstes aufheben, bevor der Besitzer des Dienstes wieder dem Cluster beitrifft und **rgmanager** neu startet.

8.4. Aktualisieren einer Konfiguration

Das Aktualisieren der Cluster-Konfiguration umfasst das Bearbeiten der Cluster-Konfigurationsdatei (`/etc/cluster/cluster.conf`) und deren Übertragung an alle Knoten im Cluster. Sie können die Konfiguration unter Verwendung einer der folgenden Verfahren aktualisieren:

- ▶ [Abschnitt 8.4.1, „Aktualisieren der Konfiguration mittels `cman_tool version -r`“](#)
- ▶ [Abschnitt 8.4.2, „Aktualisieren der Konfiguration mittels `scp`“](#)

8.4.1. Aktualisieren der Konfiguration mittels `cman_tool version -r`

Um die Konfiguration mithilfe des Befehls `cman_tool version -r` zu aktualisieren, führen Sie die folgenden Schritte aus:

1. Bearbeiten Sie auf einem beliebigen Knoten im Cluster die `/etc/cluster/cluster.conf`-Datei.
2. Aktualisieren Sie den `config_version`-Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von `config_version="2"` auf `config_version="3"`).
3. Speichern Sie die `/etc/cluster/cluster.conf` ab.
4. Führen Sie den Befehl `cman_tool version -r` aus, um die Konfiguration an die übrigen Cluster-Knoten zu verbreiten. Es ist notwendig, dass `ricci` auf jedem Cluster-Knoten ausgeführt wird, um die aktualisierten Cluster-Konfigurationsinformationen verbreiten zu können.
5. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
6. Sie können diesen Schritt (Neustart der Cluster-Software) überspringen, falls Sie nur die folgenden Konfigurationsänderungen vorgenommen haben:
 - ▶ Löschen eines Knotens aus der Cluster-Konfiguration — *es sei denn*, die Knotenanzahl verringert sich dadurch auf zwei Knoten. Informationen über das Löschen eines Knotens und die Verringerung der Knotenanzahl auf zwei Knoten finden Sie in [Abschnitt 8.2, „Hinzufügen oder Löschen eines Knotens“](#).
 - ▶ Hinzufügen eines Knotens zur Cluster-Konfiguration — *es sei denn*, die Knotenanzahl erhöht sich dadurch auf mehr als zwei Knoten. Informationen über das Hinzufügen eines Knotens und die Erhöhung der Knotenanzahl auf mehr als zwei Knoten finden Sie in [Abschnitt 8.2.2, „Einen Knoten zum Cluster hinzufügen“](#).
 - ▶ Änderungen an der Protokollierung durch Daemons.
 - ▶ Wartung von Hochverfügbarkeitsdiensten/virtuellen Maschinen (hinzufügen, bearbeiten oder löschen).
 - ▶ Wartung von Ressourcen (hinzufügen, bearbeiten oder löschen).
 - ▶ Wartung von Ausfallsicherungs-Domains (hinzufügen, bearbeiten oder löschen).

Andernfalls müssen Sie die Cluster-Software wie folgt neu starten:

- a. Stoppen Sie auf jedem Knoten die Cluster-Software gemäß [Abschnitt 8.1.2, „Stoppen der Cluster-Software“](#). Zum Beispiel:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:           [ OK ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):     [ OK ]
Unmounting GFS2 filesystem (/mnt/gfsB):     [ OK ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                     [ OK ]
clvmd terminated                            [ OK ]
[root@example-01 ~]# service cman stop
Stopping cluster:
  Leaving fence domain...                   [ OK ]
  Stopping gfs_controld...                 [ OK ]
  Stopping dlm_controld...                [ OK ]
  Stopping fenced...                      [ OK ]
  Stopping cman...                        [ OK ]
  Waiting for corosync to shutdown:       [ OK ]
  Unloading kernel modules...             [ OK ]
  Unmounting configfs...                  [ OK ]
[root@example-01 ~]#
```

- b. Starten Sie auf jedem Knoten die Cluster-Software gemäß [Abschnitt 8.1.1, „Starten der Cluster-Software“](#). Zum Beispiel:

```
[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 ~]#
```

Das Stoppen und Starten der Cluster-Software gewährleistet, dass auch solche Konfigurationsänderungen, die nur beim Start überprüft werden, in die laufende Konfiguration miteinbezogen werden.

- Führen Sie auf einem beliebigen Cluster-Knoten **cman_tools nodes** aus um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Spalte "Sts"). Zum Beispiel:

```
[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
```

- Überprüfen Sie auf einem beliebigen Knoten mithilfe des **clustat**-Dienstprogramms, ob die Hochverfügbarkeitsdienste wie erwartet funktionieren. Zusätzlich zeigt **clustat** den Status der Cluster-Knoten. Zum Beispiel:

```
[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
```

- Wenn der Cluster wie erwartet funktioniert, sind Sie mit dem Aktualisieren der Konfiguration fertig.

8.4.2. Aktualisieren der Konfiguration mittels scp

Um die Konfiguration mithilfe des **scp**-Befehls zu aktualisieren, führen Sie die folgenden Schritte aus:

- Stoppen Sie auf jedem Knoten die Cluster-Software gemäß [Abschnitt 8.1.2, „Stoppen der Cluster-](#)

[Software](#)“. Zum Beispiel:

```
[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. Bearbeiten Sie auf einem beliebigen Knoten im Cluster die `/etc/cluster/cluster.conf`-Datei.
3. Aktualisieren Sie den `config_version`-Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von `config_version="2"` auf `config_version="3"`).
4. Speichern Sie die `/etc/cluster/cluster.conf` ab.
5. Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (`cluster.rng`), indem Sie den `ccs_config_validate`-Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

6. Ist die aktualisierte Datei gültig, verwenden Sie den `scp`-Befehl, um sie auf `/etc/cluster/` in jedem Cluster-Knoten zu übertragen.
7. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
8. Starten Sie auf jedem Knoten die Cluster-Software gemäß [Abschnitt 8.1.1, „Starten der Cluster-Software“](#). Zum Beispiel:

```
[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. Führen Sie auf einem beliebigen Cluster-Knoten **cman_tools nodes** aus um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[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. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **clustat**-Dienstprogramms, ob die Hochverfügbarkeitsdienste wie erwartet funktionieren. Zusätzlich zeigt **clustat** den Status der Cluster-Knoten. Zum Beispiel:

```
[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. Wenn der Cluster wie erwartet funktioniert, sind Sie mit dem Aktualisieren der Konfiguration fertig.

Kapitel 9. Fehlerdiagnose und -behebung in einem Cluster

Cluster-Probleme können schwer zu finden und zu beheben sein, denn ein Cluster mit mehreren Systemen bringt naturgemäß ein höheres Maß an Komplexität mit sich, als dies bei der Problembehebung in einem einzelnen System der Fall ist. Allerdings gibt es bestimmte Probleme, auf die Systemadministratoren bei der Implementierung oder Verwaltung eines Clusters häufig stoßen. Wenn Sie diese häufig auftretenden Probleme und Ihre Lösungen verstehen, kann dies die Implementierung und Verwaltung Ihres Clusters deutlich vereinfachen.

Dieses Kapitel liefert Informationen über einige häufig auftretende Cluster-Probleme sowie deren Lösungen. Weiterführende Hilfe erhalten Sie entweder in unserer Wissensdatenbank oder von einem autorisierten Red Hat Support-Vertreter. Falls Ihr Problem speziell mit dem GFS2-Dateisystem zusammenhängt, können Sie dem Dokument *Global File System 2: Konfiguration und Administration* weitere Informationen über die Suche und Bereinigung von GFS2-Fehlern entnehmen.

9.1. Cluster wird nicht gebildet

Falls Sie Probleme haben, einen neuen Cluster zu bilden, überprüfen Sie Folgendes:

- ▶ Vergewissern Sie sich, dass die Namensauflösung korrekt konfiguriert ist. Der Cluster-Knotenname in der `cluster.conf`-Datei sollte mit dem Namen übereinstimmen, der zur Auflösung der Cluster-Netzwerkadresse zur Kommunikation über den Cluster verwendet wird. Falls Ihre Cluster-Knotenamen beispielsweise `nodea` und `nodeb` lauten, dann vergewissern Sie sich, dass für beide Knoten Einträge in der `/etc/cluster/cluster.conf`-Datei vorhanden sind und die `/etc/hosts`-Datei mit diesen Namen übereinstimmt.
- ▶ Da der Cluster Multicast zur Kommunikation der Knoten untereinander verwendet, stellen Sie sicher, dass auf dem Netzwerk, das der Cluster zur Kommunikation nutzt, Multicast-Datenverkehr nicht blockiert, verzögert oder anderweitig behindert wird. Beachten Sie, dass einige Cisco-Switches über Funktionen verfügen, die ggf. Verzögerungen des Multicast-Datenverkehrs verursachen.
- ▶ Verwenden Sie `telnet` oder `SSH`, um zu überprüfen, ob die entfernten Knoten erreichbar sind.
- ▶ Führen Sie den Befehl `ethtool eth1 | grep link` aus, um zu überprüfen, ob die Netzwerkverbindung aktiv ist.
- ▶ Verwenden Sie den `tcpdump`-Befehl auf jedem Knoten, um den Netzwerkverkehr zu überprüfen.
- ▶ Vergewissern Sie sich, dass keine Firewall-Regeln die Kommunikation zwischen Ihren Knoten unterbinden.
- ▶ Vergewissern Sie sich, dass die Schnittstellen, über die Sie Cluster-Datenverkehr leiten, keinen anderen Bonding-Modus außer 0 einsetzen und kein VLAN-Tagging verwenden.

9.2. Knoten können nach Fencing oder Neustart dem Cluster nicht wieder beitreten

Falls Ihre Knoten nach dem Fencing oder einem Neustart dem Cluster nicht wieder beitreten, überprüfen Sie Folgendes:

- ▶ Cluster, die Ihre Daten über einen Cisco Catalyst Switch leiten, können ggf. von diesem Problem betroffen sein.
- ▶ Vergewissern Sie sich, dass alle Cluster-Knoten dieselbe Version der `cluster.conf`-Datei verwenden. Falls die `cluster.conf`-Datei auf einem der Knoten abweicht, kann dieser Knoten dem Cluster unter Umständen nicht mehr beitreten.

Ab Red Hat Enterprise Linux 6.1 können Sie den folgenden Befehl verwenden, um zu überprüfen, ob alle in der Cluster-Konfigurationsdatei des Hosts spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen:

```
ccs -h host --checkconf
```

Für Informationen über den `ccs`-Befehl, siehe [Kapitel 5, Konfiguration des Red Hat](#)

[Hochverfügbarkeits-Add-Ons mit dem `ccs`-Befehl](#) und [Kapitel 6, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit `ccs`](#).

- ▶ Stellen Sie sicher, dass Sie **chkconfig on** für die Cluster-Dienste in dem Knoten konfiguriert haben, der dem Cluster beizutreten versucht.
- ▶ Vergewissern Sie sich, dass keine Firewall-Regeln die Kommunikation zwischen den Knoten im Cluster unterbinden.

9.3. Cluster-Dienste hängen sich auf

Wenn die Cluster-Dienste einen Knoten abzugrenzen versuchen, stoppen die Cluster-Dienste, bis die Fencing-Operation erfolgreich abgeschlossen wurde. Falls sich also Ihr Cluster-verwalteter Speicher oder Dienst aufhängt und die Cluster-Knoten unterschiedliche Ansichten der Cluster-Mitgliedschaft zeigen, oder falls Sie einen Knoten abzugrenzen versuchen und Sie zur Wiederherstellung Knoten neu starten müssen, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- ▶ Der Cluster hat ggf. versucht, einen Knoten abzugrenzen, und diese Fencing-Operation kann unter Umständen fehlgeschlagen sein.
- ▶ Sehen Sie sich die `/var/log/messages`-Datei auf allen Knoten an und suchen Sie nach Nachrichten bezüglich einer fehlgeschlagenen Abgrenzung. Sollten Sie welche finden, starten Sie die Knoten im Cluster neu und konfigurieren Sie das Fencing korrekt.
- ▶ Vergewissern Sie sich, dass keine Aufspaltung des Netzwerks auftrat, wie in [Abschnitt 9.6, „Jeder Knoten in einem Zwei-Knoten-Cluster meldet den jeweils anderen Knoten als ausgefallen“](#) beschrieben, und stellen Sie sicher, dass die Kommunikation zwischen den Knoten nach wie vor möglich ist und das Netzwerk aktiv ist.
- ▶ Falls Knoten den Cluster verlassen, verfügen die verbleibenden Knoten ggf. über kein Quorum mehr. Der Cluster braucht jedoch ein Quorum, um funktionsfähig zu sein. Falls Knoten entfernt werden, so dass der Cluster nicht länger über ein Quorum verfügt, hängen sich Dienste und Speicher auf. Passen Sie entweder die erwarteten Stimmen an oder fügen Sie dem Cluster wieder die benötigte Anzahl an Knoten hinzu.



Anmerkung

Sie können einen Knoten manuell mit dem `fence_node`-Befehl oder mit **Conga** abgrenzen. Für Informationen diesbezüglich, siehe `fence_node`-Handbuchseite und [Abschnitt 4.2.2, „Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen“](#).

9.4. Cluster-Dienst startet nicht

Falls ein Cluster-verwalteter Dienst nicht startet, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- ▶ Die Dienstkonfiguration in der `cluster.conf`-Datei enthält unter Umständen Syntaxfehler. Führen Sie den `rg_test`-Befehl aus, um die Syntax in Ihrer Konfiguration zu überprüfen. Falls diese Konfigurations- oder Syntaxfehler enthält, wird `rg_test` Sie über das Problem informieren.

```
$ rg_test test /etc/cluster/cluster.conf start service servicename
```

Für weitere Informationen über den `rg_test`-Befehl, siehe [Abschnitt C.5, „Testen und Fehlerbehebung von Diensten und der Ressourcenreihenfolge“](#).

Ist die Konfiguration gültig, erhöhen Sie als Nächstes die Protokollierung des Ressourcengruppenmanagers und untersuchen die Protokolle, um Hinweise darauf zu erhalten, warum der Dienst nicht startet. Sie können die Protokollierungsstufe erhöhen, indem Sie den Parameter `loglevel="7"` zum `rm`-Tag in der `cluster.conf`-Datei hinzufügen. Dadurch erhalten Sie ausführlichere Protokollmeldungen hinsichtlich dem Starten, Stoppen und Migrieren von geclusterten Diensten.

9.5. Migration von Cluster-verwalteten Diensten schlägt fehl

Falls die Migration eines Cluster-verwalteten Dienstes auf einen anderen Knoten fehlschlägt, der Dienst jedoch auf einem bestimmten Knoten startet, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- ▶ Vergewissern Sie sich, dass die Ressourcen, die zum Ausführen eines bestimmten Dienstes notwendig sind, auf allen Knoten im Cluster vorhanden sind, die unter Umständen diesen Dienst ausführen müssen. Falls Ihr geclusterter Dienst beispielsweise eine Skriptdatei an einem bestimmten Speicherort voraussetzt oder ein Dateisystem an einem bestimmten Einhängeort erwartet, dann müssen Sie sicherstellen, dass diese Ressourcen auf allen Knoten im Cluster an den erwarteten Orten vorliegen.
- ▶ Vergewissern Sie sich, dass Ausfallsicherungs-Domains, Dienstabhängigkeiten und Dienstexklusivität nicht derart konfiguriert sind, dass infolgedessen eine Migration von Diensten auf Knoten nicht erwartungsgemäß funktionieren kann.
- ▶ Falls es sich bei dem fraglichen Dienst um eine virtuelle Maschinenressource handelt, prüfen Sie die Dokumentation um sicherzustellen, dass Sie alle notwendigen Konfigurationen korrekt vorgenommen haben.
- ▶ Erhöhen Sie die Protokollierung des Ressourcengruppenmanagers wie in [Abschnitt 9.4, „Cluster-Dienst startet nicht“](#) beschrieben, und untersuchen Sie die Protokolle, um Hinweise darauf zu erhalten, warum die Migration des Dienstes fehlschlägt.

9.6. Jeder Knoten in einem Zwei-Knoten-Cluster meldet den jeweils anderen Knoten als ausgefallen

Falls es sich bei Ihrem Cluster um einen Zwei-Knoten-Cluster handelt und jeder Knoten meldet, dass er läuft, der jeweils andere Knoten jedoch angeblich ausgefallen ist, dann deutet dies darauf hin, dass die beiden Knoten nicht über Multicast oder über das Cluster-Heartbeat-Netzwerk miteinander kommunizieren können. Dieser Zustand der Netzwerkaufspaltung wird "Split Brain" genannt. Um dies zu beheben, folgen Sie den Hinweisen in [Abschnitt 9.1, „Cluster wird nicht gebildet“](#).

9.7. Knoten werden nach LUN-Pfad-Ausfall abgegrenzt

Wenn ein oder mehrere Knoten in Ihrem Cluster abgegrenzt werden, wenn ein LUN-Pfad-Ausfall auftritt, kann dies daran liegen, dass eine Quorum-Platte statt Multipath-Speicher verwendet wird. Falls Sie eine Quorum-Platte verwenden und diese über Multipath-Speicher liegt, dann vergewissern Sie sich, dass Sie sämtliche Zeitangaben und Zeitüberschreitungen korrekt eingestellt haben, um einen Pfadausfall tolerieren zu können.

9.8. Quorum-Platte erscheint nicht als Cluster-Mitglied

Falls Sie Ihr System zur Verwendung einer Quorum-Platte konfiguriert haben, diese jedoch nicht als Mitglied im Cluster erscheint, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- ▶ Vergewissern Sie sich, dass Sie **chkconfig on** für den **qdisk**-Dienst festgelegt haben.
- ▶ Vergewissern Sie sich, dass Sie den **qdisk**-Dienst gestartet haben.
- ▶ Beachten Sie, dass es einige Minuten dauern kann, bis sich die Quorum-Platte beim Cluster registriert hat. Dies ist normales und erwartetes Verhalten.

9.9. Ungewöhnliches Verhalten bei Ausfallsicherung

Ein häufig auftretendes Problem mit Cluster-Servern ist ungewöhnliches Verhalten bei der Ausfallsicherung. Dienste stoppen, wenn andere Dienste starten, oder Dienste starten nicht auf einem anderen Knoten. Die Ursache hierfür kann in den komplexen Systemen zur Ausfallsicherung liegen, bestehend aus Ausfallsicherungs-Domains, Dienstabhängigkeiten und Dienstexklusivitäten. Versuchen

Sie, Ihre Dienst- oder Ausfallsicherungskonfiguration zu vereinfachen, und testen Sie dann, ob das Problem weiterhin besteht. Vermeiden Sie Dienstexklusivität und -abhängigkeiten, wenn Sie sich nicht absolut sicher sind, wie diese Features die Ausfallsicherung unter allen denkbaren Bedingungen beeinflussen.

9.10. Wahlloses Fencing

Falls Sie feststellen, dass ein Knoten wahllos abgegrenzt wird, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- ▶ Die Ursache für das Fencing ist *immer* ein Knoten, der die Kommunikation mit dem Rest des Clusters abgebrochen hat und keinen "Heartbeat" mehr überträgt.
- ▶ Jede Situation, die dazu führt, dass ein System innerhalb einer festgelegten Zeitspanne keinen Heartbeat überträgt, kann die Abgrenzung verursachen. Standardmäßig beträgt diese Zeitspanne 10 Sekunden. Sie können diese Zeitspanne festlegen, indem Sie den gewünschten Wert (in Millisekunden) an den Token-Parameter des Totem-Tags in der **cluster.conf**-Datei hinzufügen (z.B. **totem token="30000"** für 30 Sekunden).
- ▶ Vergewissern Sie sich, dass das Netzwerk einwandfrei funktioniert.
- ▶ Vergewissern Sie sich, dass kein ungewöhnlicher Bonding-Modus oder VLAN-Tagging auf den Schnittstellen eingesetzt wird, die vom Cluster zur Kommunikation der Knoten untereinander verwendet werden.
- ▶ Führen Sie Maßnahmen durch um festzustellen, ob das System sich aufhängt oder ob eine Kernel-Panik auftritt. Richten Sie das **kdump**-Dienstprogramm ein, um einen Speicherauszug während einer dieser wahllosen Abgrenzungen zu erhalten.
- ▶ Stellen Sie sicher, dass Sie die auftretende Situation nicht fälschlicherweise für eine Abgrenzung halten, obwohl es ggf. zum Beispiel die Quorum-Platte ist, die aufgrund eines Speicherausfalls einen Knoten ausschließt, oder ein Produkt eines Drittanbieters wie Oracle RAC, das einen Knoten aus anderen Gründen neu startet. Die Nachrichtenprotokolle sind oft hilfreich, um diese Probleme zu untersuchen. Bei jeder Abgrenzung oder jedem Knoten-Neustart sollten Sie standardmäßig die Nachrichtenprotokolle vom Zeitpunkt der Abgrenzung/des Neustarts auf allen Knoten im Cluster überprüfen.
- ▶ Überprüfen Sie das System zudem gründlich auf Hardware-Fehler, die dazu führen könnten, dass das System nicht erwartungsgemäß auf Heartbeats reagiert.

Kapitel 10. SNMP-Konfiguration mit dem Red Hat Hochverfügbarkeits-Add-On

Ab der Red Hat Enterprise Linux 6.1 Release bietet das Red Hat Hochverfügbarkeits-Add-On Unterstützung für SNMP-Traps. Dieses Kapitel beschreibt, wie Sie Ihr System für SNMP konfigurieren können, gefolgt von einer Zusammenfassung der Traps, die das Red Hat Hochverfügbarkeits-Add-On für bestimmte Cluster-Ereignisse ausgibt.

10.1. SNMP und das Red Hat Hochverfügbarkeits-Add-On

Der Red Hat Hochverfügbarkeits-Add-On SNMP-Subagent ist **foghorn**, der die SNMP-Traps ausgibt. Der **foghorn**-Subagent kommuniziert mit dem **snmpd**-Daemon über das AgentX-Protokoll. Der **foghorn**-Subagent erstellt lediglich SNMP-Traps; er unterstützt keine anderen SNMP-Operationen wie z.B. **get** oder **set**.

Es gibt derzeit keine **config**-Optionen für den **foghorn**-Subagent. Er kann nicht zur Verwendung eines bestimmten Sockets konfiguriert werden; nur der standardmäßige AgentX-Socket wird derzeit unterstützt.

10.2. Konfiguration von SNMP mit dem Red Hat Hochverfügbarkeits-Add-On

Um SNMP für das Red Hat Hochverfügbarkeits-Add-On zu konfigurieren, führen Sie die folgenden Schritte auf jedem Knoten im Cluster aus, um sicherzustellen, dass die nötigen Dienste aktiviert sind und ausgeführt werden.

1. Um SNMP-Traps mit dem Red Hat Hochverfügbarkeits-Add-On zu verwenden, ist der **snmpd**-Dienst erforderlich, der als Master-Agent fungiert. Da der **foghorn**-Dienst der Subagent ist und das AgentX-Protokoll verwendet, müssen Sie die folgende Zeile zur **/etc/snmp/snmpd.conf**-Datei hinzufügen, um AgentX-Unterstützung zu aktivieren:

```
master agentx
```

2. Um den Host festzulegen, an den die SNMP-Trap-Benachrichtigungen gesendet werden sollen, fügen Sie die folgende Zeile zur **/etc/snmp/snmpd.conf**-Datei hinzu:

```
trap2sink host
```

Weitere Informationen über die Handhabung der Benachrichtigungen finden Sie auf der **snmpd.conf**-Handbuchseite.

3. Vergewissern Sie sich, dass der **snmpd**-Daemon aktiviert ist und läuft, indem Sie die folgenden Befehle ausführen:

```
% chkconfig snmpd on  
% service snmpd start
```

4. Falls der **messagebus**-Daemon noch nicht aktiviert ist und noch nicht läuft, führen Sie die folgenden Befehle aus:

```
% chkconfig messagebus on  
% service messagebus start
```

5. Vergewissern Sie sich, dass der **foghorn**-Daemon aktiviert ist und läuft, indem Sie die folgenden Befehle ausführen:

```
% chkconfig foghorn on  
% service foghorn start
```

6. Führen Sie den folgenden Befehl aus, um Ihr System so zu konfigurieren, dass der **COROSYNC-MIB** SNMP-Traps generiert und um sicherzustellen, dass der **corosync-notifyd**-Daemon aktiviert ist und läuft:

```
$ echo "OPTIONS=\"-d\" " > /etc/sysconfig/corosync-notifyd
$ chkconfig corosync-notifyd on
$ service corosync-notifyd start
```

Nachdem Sie jeden Knoten im Cluster für SNMP konfiguriert haben und sichergestellt haben, dass die nötigen Dienste laufen, werden D-bus Signale nunmehr vom **foghorn**-Dienst empfangen und in SNMPv2-Traps übersetzt. Diese Traps werden anschließend an den Host übertragen, den Sie mit dem **trapsink**-Eintrag zum Empfang von SNMPv2-Traps definiert haben.

10.3. Weiterleiten von SNMP-Traps

Es ist möglich, SNMP-Traps an eine Maschine außerhalb des Clusters weiterzuleiten, auf der Sie den **snmptrapd**-Daemon einsetzen und anpassen können, wie die Benachrichtigungen gehandhabt werden sollen.

Um SNMP-Traps in einem Cluster auf eine Maschine außerhalb des Clusters weiterzuleiten, führen Sie die folgenden Schritte aus:

1. Folgen Sie für jeden Knoten im Cluster dem in [Abschnitt 10.2, „Konfiguration von SNMP mit dem Red Hat Hochverfügbarkeits-Add-On“](#) beschriebenen Verfahren, und geben Sie dabei im **trap2sink host**-Eintrag in der **/etc/snmp/snmpd.conf**-Datei den externen Host an, auf dem der **snmptrapd**-Daemon ausgeführt werden soll.
2. Bearbeiten Sie auf dem externen Host, der die Traps empfangen wird, die **/etc/snmp/snmptrapd.conf** Konfigurationsdatei, um Ihre Community-Strings festzulegen. Beispielsweise können Sie den folgenden Eintrag verwenden, um es dem **snmptrapd**-Daemon zu ermöglichen, Benachrichtigungen unter Verwendung des **public** Community-Strings zu verarbeiten.

```
authCommunity log,execute,net public
```

3. Vergewissern Sie sich auf dem externen Host, der die Traps empfangen wird, dass der **snmptrapd**-Daemon aktiviert ist und läuft, indem Sie die folgenden Befehle ausführen:

```
% chkconfig snmptrapd on
% service snmptrapd start
```

Werfen Sie für weitere Informationen über die Verarbeitung von SNMP-Benachrichtigungen einen Blick auf die **snmptrapd.conf**-Handbuchseite.

10.4. SNMP-Traps generiert vom Red Hat Hochverfügbarkeits-Add-On

Der **foghorn**-Daemon generiert die folgenden Traps:

► fenceNotifyFenceNode

Diese Trap tritt auf, wenn ein abgegrenzter Knoten versucht, einen anderen Knoten abzugrenzen. Beachten Sie, dass diese Trap nur auf einem Knoten generiert wird - auf demjenigen Knoten, der die Fencing-Operation durchzuführen versucht. Die Benachrichtigung beinhaltet die folgenden Felder:

- **fenceNodeName** - Name des abgegrenzten Knotens
- **fenceNodeID** - Knoten-ID des abgegrenzten Knotens
- **fenceResult** - das Ergebnis der Fencing-Operation (0 falls erfolgreich, -1 falls Fehler auftraten, -2 falls keine Fencing-Methoden definiert sind)

► **rgmanagerServiceStateChange**

Diese Trap tritt auf, wenn sich der Status eines Cluster-Dienstes ändert. Die Benachrichtigung beinhaltet die folgenden Felder:

- **rgmanagerServiceName** - der Name des Dienstes einschließlich Diensttyp (z.B. **service:foo** oder **vm:foo**).
- **rgmanagerServiceState** - der Status des Dienstes. Davon ausgenommen sind Übergangszustände wie **starting** und **stopping**, um die Traps übersichtlich zu halten.
- **rgmanagerServiceFlags** - die Dienst-Flags. Derzeit gibt es zwei unterstützte Flags: **frozen**, was einen Dienst kennzeichnet, der mithilfe des Befehls **clusvcadm -Z** eingefroren wurde, und **partial**, was einen Dienst kennzeichnet, in dem eine ausgefallene Ressource als **non-critical** markiert wurde, so dass die Ressource ausfallen und deren Komponenten manuell neu gestartet werden können, ohne dass der gesamte Dienst davon betroffen ist.
- **rgmanagerServiceCurrentOwner** - der Dienstbesitzer. Falls der Dienst nicht läuft, ist dies (**none**).
- **rgmanagerServicePreviousOwner** - der letzte Dienstbesitzer, sofern bekannt. Ist der letzte Dienstbesitzer nicht bekannt, ist dies ggf. (**none**).

Der **corosync-nodifyd**-Daemon generiert die folgenden Traps:

► **corosyncNoticesNodeStatus**

Diese Trap tritt auf, wenn ein Knoten einem Cluster beitrifft oder diesen verlässt. Die Benachrichtigung beinhaltet die folgenden Felder:

- **corosyncObjectsNodeName** - Knotenname
- **corosyncObjectsNodeID** - Knoten-ID
- **corosyncObjectsNodeAddress** - Knoten-IP-Adresse
- **corosyncObjectsNodeStatus** - Knotenstatus (**joined** oder **left**)

► **corosyncNoticesQuorumStatus**

Diese Trap tritt auf, wenn sich der Quorumstatus ändert. Die Benachrichtigung beinhaltet die folgenden Felder:

- **corosyncObjectsNodeName** - Knotenname
- **corosyncObjectsNodeID** - Knoten-ID
- **corosyncObjectsQuorumStatus** - neuer Status des Quorum (**quorate** oder **NOT quorate**)

► **corosyncNoticesAppStatus**

Diese Trap tritt auf, wenn eine Client-Applikation eine Verbindung mit Corosync herstellt oder diese unterbricht.

- **corosyncObjectsNodeName** - Knotenname
- **corosyncObjectsNodeID** - Knoten-ID
- **corosyncObjectsAppName** - Applikationsname
- **corosyncObjectsAppStatus** - neuer Status einer Applikation (**connected** oder **disconnected**)

Parameter der Fencing-Geräte

Dieser Anhang enthält Tabellen mit Beschreibungen der Fencing-Geräteparameter sowie den Namen des Fencing-Agents für die jeweiligen Geräte.



Anmerkung

Der **Name**-Parameter für ein Fencing-Gerät spezifiziert einen beliebigen Namen für das Gerät, der von dem Red Hat Hochverfügbarkeits-Add-On verwendet wird. Es handelt sich hierbei nicht um den DNS-Namen für das Gerät.



Anmerkung

Bestimmte Fencing-Geräte haben einen optionalen **Password Script**-Parameter. Mithilfe des **Password Script**-Parameters können Sie festlegen, dass ein Fencing-Gerätepasswort von einem Skript zur Verfügung gestellt wird, anstatt vom **Password**-Parameter. Die Verwendung des **Password Script**-Parameters ersetzt den **Password**-Parameter und ermöglicht, dass Passwörter in der Cluster-Konfigurationsdatei (`/etc/cluster/cluster.conf`) nicht sichtbar sind.

Tabelle A.1. APC Power Switch (telnet/SSH)

| Feld | Beschreibung |
|-------------------------------|---|
| Name | Ein Name für das mit dem Cluster verbundene APC-Gerät, bei dem sich der Fencing-Daemon über telnet/ssh anmeldet. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| Switch (optional) | Die Switch-Nummer für den APC-Switch, der mit dem Knoten verbindet, wenn Sie mehrere in Reihe geschaltete Switches haben. |
| Use SSH | Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. |
| Path to the SSH identity file | Die Identitätsdatei für SSH. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| fence_apc | Der Fencing-Agent für APC über telnet/SSH. |

Tabelle A.2. Brocade Fabric Switch

| Feld | Beschreibung |
|----------------------------|--|
| Name | Ein Name für das mit dem Cluster verbundene Brocade-Gerät. |
| IP-Adresse | Die IP-Adresse des Geräts. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Port | Die Switch-Outlet-Nummer. |
| fence_brocade | Der Fencing-Agent für Brocade FC Switches. |

Tabelle A.3. APC Power Switch über SNMP

| Feld | Beschreibung |
|--------------------------------|---|
| Name | Ein Name für das mit dem Cluster verbundene APC-Gerät, bei dem sich der Fencing-Daemon über das SNMP-Protokoll anmeldet. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| UDP/TCP port | Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| Switch (optional) | Die Switch-Nummer für den APC-Switch, der mit dem Knoten verbindet, wenn Sie mehrere in Reihe geschaltete Switches haben. |
| SNMP version | Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1. |
| SNMP community | Der SNMP-Community-String; der Standardwert ist private . |
| SNMP security level | Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv). |
| SNMP authentication protocol | Das SNMP-Authentifizierungsprotokoll (MD5, SHA). |
| SNMP privacy protocol | Das SNMP-Verschlüsselungsprotokoll (DES, AES). |
| SNMP privacy protocol password | Das Passwort für das SNMP-Verschlüsselungsprotokoll. |
| SNMP privacy protocol script | Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den SNMP privacy protocol password -Parameter. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| fence_apc_snmp | Der Fencing-Agent für APC, der sich über das SNMP-Protokoll beim SNMP-Gerät anmeldet. |

Tabelle A.4. Cisco UCS

| Feld | Beschreibung |
|----------------------------|--|
| Name | Ein Name für das Cisco UCS-Gerät. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| SSL | Die SSL-Verbindung. |
| IP port (optional) | Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| Power timeout | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten auf eine Statusänderung geprüft werden soll. |
| Shell timeout | Anzahl von Sekunden, die nach einem Befehl auf eine Eingabeaufforderung gewartet werden soll. |
| Retry on | Anzahl der erneuten Versuche zum Anschalten. |
| fence_cisco_ucs | Der Fencing-Agent für Cisco UCS. |

Tabelle A.5. Cisco MDS

| Feld | Beschreibung |
|--------------------------------|---|
| Name | Ein Name für das Cisco MDS 9000 Series Gerät mit aktiviertem SNMP. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| SNMP version | Die zu verwendende SNMP-Version (1, 2c, 3). |
| SNMP community | Der SNMP-Community-String. |
| SNMP authentication protocol | Das SNMP-Authentifizierungsprotokoll (MD5, SHA). |
| SNMP security level | Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv). |
| SNMP privacy protocol | Das SNMP-Verschlüsselungsprotokoll (DES, AES). |
| SNMP privacy protocol password | Das Passwort für das SNMP-Verschlüsselungsprotokoll. |
| SNMP privacy protocol script | Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den SNMP privacy protocol password -Parameter. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| fence_cisco_mds | Der Fencing-Agent für Cisco MDS. |

Tabelle A.6. Dell DRAC 5

| Feld | Beschreibung |
|-------------------------------|--|
| Name | Der dem DRAC zugewiesene Name. |
| IP-Adresse | Die IP-Adresse oder der Hostname für den DRAC. |
| IP port (optional) | Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port. |
| Login | Der Login-Name für den Zugriff auf den DRAC. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem DRAC. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Module name | (optional) Der Modulname für den DRAC, wenn Sie mehrere DRAC-Module haben. |
| Use SSH | Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. |
| Path to the SSH identity file | Die Identitätsdatei für SSH. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| fence_drac5 | Der Fencing-Agent für Dell DRAC 5. |

Tabelle A.7. Egenera SAN-Controller

| Feld | Beschreibung |
|---------------------|---|
| Name | Ein Name für das mit dem Cluster verbundene eGenera BladeFrame-Gerät. |
| CServer | Der dem Gerät zugewiesene Hostname (und optional der Benutzername in der Form username@hostname). Siehe fence_egera(8) Handbuchseite für weitere Informationen. |
| ESH Path (optional) | Der Pfad zum esh-Befehl auf dem cserver (Standard ist /opt/panmgr/bin/esh) |
| lpan | Das Logical Process Area Network (LPAN) des Geräts. |
| pserver | Der Name des Processing Blade (pserver) des Geräts. |
| fence_egera | Der Fencing-Agent für das eGenera BladeFrame. |

Tabelle A.8. ePowerSwitch

| Feld | Beschreibung |
|----------------------------|--|
| Name | Ein Name für das mit dem Cluster verbundene ePowerSwitch-Gerät. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| Hidden page | Der Name der Hidden Page für das Gerät. |
| fence_eps | Der Fencing-Agent für ePowerSwitch. |

Tabelle A.9. Fujitsu Siemens Remoteview Service Board (RSB)

| Feld | Beschreibung |
|----------------------------|--|
| Name | Ein Name des RSB, das als Fencing-Gerät verwendet werden soll. |
| Hostname | Der Hostname des Geräts. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| TCP-Port | Die Port-Nummer, auf dem der telnet-Dienst horcht. |
| fence_rsb | Der Fencing-Agent für Fujitsu-Siemens RSB. |

Tabelle A.10. Fence virt

| Feld | Beschreibung |
|-----------------------|---|
| Name | Ein Name für das Fence virt Fencing-Gerät. |
| Port | Die abzugrenzende virtuelle Maschine (Domain-UUID oder Name). |
| Serial device | Auf dem Host muss das serielle Gerät in der Konfigurationsdatei einer jeden Domain zugewiesen sein. Werfen Sie für weitere Informationen einen Blick auf die fence_virt.conf -Handbuchseite. Ist dieses Feld angegeben, veranlasst dies den fence_virt -Fencing-Agent zum Betrieb im seriellen Modus. Wird kein Wert angegeben, veranlasst dies den fence_virt -Fencing-Agent zum Betrieb im VM-Channel-Modus. |
| Serial parameters | Die seriellen Parameter. Der Standard ist 115200, 8N1. |
| VM channel IP address | Die Channel-IP. Der Standardwert ist 10.0.2.179. |
| Channel port | Der Channel-Port. Der Standardwert ist 1229. |
| fence_virt | Der Fencing-Agent für ein Fence-virt Fencing-Gerät. |

Tabelle A.11. HP iLO/iLO2 (Integrated Lights Out)

| Feld | Beschreibung |
|----------------------------|--|
| Name | Ein Name für den Server mit HP iLO Unterstützung. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| IP port (optional) | Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| fence_ilo | Der Fencing-Agent für HP iLO Geräte. |

Tabelle A.12. HP iLO (Integrated Lights Out) MP

| Feld | Beschreibung |
|-------------------------------|--|
| Name | Ein Name für den Server mit HP iLO Unterstützung. |
| Hostname | Der Hostname des Geräts. |
| IP port (optional) | Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| SSH | Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. |
| Path to the SSH identity file | Die Identitätsdatei für SSH. |
| Force command prompt | Der zu verwendende Befehls-Prompt. Der Standardwert ist 'MP>', 'hpiLO->'. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| fence_ilo_mp | Der Fencing-Agent für HP iLO MP Geräte. |

Tabelle A.13. IBM BladeCenter

| Feld | Beschreibung |
|-------------------------------|--|
| Name | Ein Name für das mit dem Cluster verbundene IBM BladeCenter-Gerät. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| IP port (optional) | Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| Use SSH | Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. |
| Path to the SSH identity file | Die Identitätsdatei für SSH. |
| fence_bladecenter | Der Fencing-Agent für IBM BladeCenter. |

Tabelle A.14. IBM BladeCenter SNMP

| Feld | Beschreibung |
|--------------------------------|---|
| Name | Ein Name für das mit dem Cluster verbundene IBM BladeCenter SNMP-Gerät. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| UDP/TCP port (optional) | Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| SNMP version | Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1. |
| SNMP community | Der SNMP-Community-String. |
| SNMP security level | Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv). |
| SNMP authentication protocol | Das SNMP-Authentifizierungsprotokoll (MD5, SHA). |
| SNMP privacy protocol | Das SNMP-Verschlüsselungsprotokoll (DES, AES). |
| SNMP privacy protocol password | Das Passwort für das SNMP-Verschlüsselungsprotokoll. |
| SNMP privacy protocol script | Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den SNMP privacy protocol password -Parameter. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| fence_bladecenter | Der Fencing-Agent für IBM BladeCenter. |

Tabelle A.15. IF MIB

| Feld | Beschreibung |
|--------------------------------|---|
| Name | Ein Name für das mit dem Cluster verbundene IF MIB-Gerät. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| UDP/TCP port (optional) | Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| SNMP version | Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1. |
| SNMP community | Der SNMP-Community-String. |
| SNMP security level | Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv). |
| SNMP authentication protocol | Das SNMP-Authentifizierungsprotokoll (MD5, SHA). |
| SNMP privacy protocol | Das SNMP-Verschlüsselungsprotokoll (DES, AES). |
| SNMP privacy protocol password | Das Passwort für das SNMP-Verschlüsselungsprotokoll. |
| SNMP privacy protocol script | Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den SNMP privacy protocol password -Parameter. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| fence_ifmib | Der Fencing-Agent für IF-MIB Geräte. |

Tabelle A.16. Intel Modular

| Feld | Beschreibung |
|--------------------------------|---|
| Name | Ein Name für das mit dem Cluster verbundene Intel Modular-Gerät. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| SNMP version | Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1. |
| SNMP community | Der SNMP-Community-String; der Standardwert ist private . |
| SNMP security level | Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv). |
| SNMP authentication protocol | Das SNMP-Authentifizierungsprotokoll (MD5, SHA). |
| SNMP privacy protocol | Das SNMP-Verschlüsselungsprotokoll (DES, AES). |
| SNMP privacy protocol password | Das Passwort für das SNMP-Verschlüsselungsprotokoll. |
| SNMP privacy protocol script | Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den SNMP privacy protocol password -Parameter. |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| fence_intelmodular | Der Fencing-Agent für APC. |

Tabelle A.17. IPMI (Intelligent Platform Management Interface) LAN

| Feld | Beschreibung |
|----------------------------|--|
| Name | Ein Name für das mit dem Cluster verbundene IPMI LAN Gerät. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| Login | Der Login-Name eines Benutzers, der Befehle zum An- und Ausschalten des angegebenen IPMI-Ports ausgeben darf. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem IPMI-Port. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Authentication Type | none , password , md2 oder md5 |
| Use Lanplus | True oder 1 . Falls leer, lautet der Wert False . |
| Ciphersuite to use | Die Remote-Server-Authentifizierung, Integrität und Verschlüsselungsalgorithmen, die für IPMIv2 lanplus Verbindungen verwendet werden. |
| fence_ipmilan | Der Fencing-Agent für Maschinen, die durch IPMI gesteuert werden. |

Tabelle A.18. SCSI Fencing

| Feld | Beschreibung |
|-------------------|--|
| Name | Ein Name für das SCSI-Fencing-Gerät. |
| Node name | Name des abzugrenzenden Knotens. Siehe fence_scsi(8) Handbuchseite für weitere Informationen. |
| fence_scsi | Der Fencing-Agent für SCSI persistente Reservierungen. |

**Anmerkung**

Die Verwendung von SCSI persistenten Reservierungen als Fencing-Methode wird zwar unterstützt, unterliegt jedoch den folgenden Einschränkungen:

- Bei der Verwendung von SCSI-Fencing müssen sich alle Knoten im Cluster bei demselben Gerät registrieren, damit jeder Knoten den Registrierungsschlüssel eines anderen Knotens von allen Geräten entfernen kann, bei denen er registriert ist.
- Bei den Geräten, die als Cluster-Datenträger eingesetzt werden, sollte es sich um komplette LUNs handeln, nicht um Partitionen. SCSI persistente Reservierungen arbeiten auf einer gesamten LUN, was bedeutet, dass der Zugriff auf jede LUN kontrolliert wird, nicht auf einzelne Partitionen.

Tabelle A.19. WTI Power Switch

| Feld | Beschreibung |
|-------------------------------|--|
| Name | Ein Name für den mit dem Cluster verbundenen WTI Power Switch. |
| IP-Adresse | Die IP-Adresse oder der Hostname des Geräts. |
| IP port (optional) | Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port. |
| Login | Der Login-Name für den Zugriff auf das Gerät. |
| Password | Das Passwort zur Authentifizierung der Verbindung mit dem Gerät. |
| Password Script (optional) | Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den Password -Parameter. |
| Port | Physische Anschlussnummer oder Name der virtuellen Maschine. |
| Force command prompt | Der zu verwendende Befehls-Prompt. Der Standardwert ist ['RSM>', '>MPC', 'IPS>', 'TPS>', 'NBB>', 'NPS>', 'VMR>'] |
| Power wait | Anzahl von Sekunden, die nach einem Befehl zum An- oder Abschalten gewartet werden soll. |
| Use SSH | Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. |
| Path to the SSH identity file | Die Identitätsdatei für SSH. |
| fence_wti | Der Fencing-Agent für den WTI Network Power Switch. |

Parameter der Hochverfügbarkeitsressourcen

Dieser Anhang beschreibt die Parameter der Hochverfügbarkeitsressource. Sie können diese Parameter mithilfe von **Luci** oder unter Verwendung des **ccs**-Befehls konfigurieren, oder indem Sie **etc/cluster/cluster.conf** bearbeiten. [Tabelle B.1, „Hochverfügbarkeitsressourcen-Übersicht“](#) listet die Ressourcen auf, ihre zugehörigen Ressourcen-Agents, sowie Verweise auf andere Tabellen mit Parameterbeschreibungen. Für ein besseres Verständnis von Ressourcen-Agents können Sie sich diese in **/usr/share/cluster** in jedem beliebigen Cluster-Knoten ansehen.

Eine vollständige Liste samt Beschreibung aller **cluster.conf**-Elemente und -Parameter finden Sie im Cluster-Schema unter **/usr/share/cluster/cluster.rng** und dem annotierten Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (zum Beispiel **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Tabelle B.1. Hochverfügbarkeitsressourcen-Übersicht

| Ressource | Ressourcen-Agent | Verweis auf Parameterbeschreibung |
|--------------------|------------------|---|
| Apache | apache.sh | Tabelle B.2, „Apache Server“ |
| Dateisystem | fs.sh | Tabelle B.3, „Dateisystem“ |
| GFS2-Dateisystem | clusterfs.sh | Tabelle B.4, „GFS2“ |
| IP-Adresse | ip.sh | Tabelle B.5, „IP-Adresse“ |
| LVM | lvm.sh | Tabelle B.6, „LVM“ |
| MySQL | mysql.sh | Tabelle B.7, „MySQL®“ |
| NFS Client | nfsclient.sh | Tabelle B.8, „NFS Client“ |
| NFS Export | nfsexport.sh | Tabelle B.9, „NFS Export“ |
| NFS/CIFS Mount | netfs.sh | Tabelle B.10, „NFS/CIFS Mount“ |
| Open LDAP | openldap.sh | Tabelle B.11, „Open LDAP“ |
| Oracle 10g | oracledb.sh | Tabelle B.12, „Oracle® 10g“ |
| PostgreSQL 8 | postgres-8.sh | Tabelle B.13, „PostgreSQL 8“ |
| SAP-Datenbank | SAPDatabase | Tabelle B.14, „SAP®-Datenbank“ |
| SAP-Instanz | SAPInstance | Tabelle B.15, „SAP®-Instanz“ |
| Samba | samba.sh | Tabelle B.16, „Samba-Dienst“ |
| Skript | script.sh | Tabelle B.17, „Skript“ |
| Dienst | service.sh | Tabelle B.18, „Dienst“ |
| Sybase ASE | ASEHAagent.sh | Tabelle B.19, „Sybase® ASE-Ausfallsicherungsinstanz“ |
| Tomcat 6 | tomcat-6.sh | Tabelle B.20, „Tomcat 6“ |
| Virtuelle Maschine | vm.sh | Tabelle B.21, „Virtuelle Maschine“ ANMERKUNG: Luci zeigt dies als virtuellen Dienst an, falls der Host-Cluster virtuelle Maschinen unterstützt. |

Tabelle B.2. Apache Server

| Feld | Beschreibung |
|-------------------------|--|
| Name | Der Name des Apache-Dienstes. |
| Server Root | Der Standardwert ist <code>/etc/httpd</code> . |
| Config File | Spezifiziert die Apache-Konfigurationsdatei. Der Standardwert ist <code>/etc/httpd/conf</code> . |
| httpd Options | Weitere Befehlszeilenoptionen für <code>httpd</code> . |
| Shutdown Wait (seconds) | Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird. |

Tabelle B.3. Dateisystem

| Feld | Beschreibung |
|-----------------------------------|---|
| Name | Spezifiziert einen Namen für die Dateisystemressource. |
| File System Type | Falls nicht angegeben, versucht <code>mount</code> , den Dateisystemtyp zu bestimmen. |
| Mount Point | Pfad in der Dateisystemhierarchie, unter dem dieses Dateisystem eingehängt wird. |
| Device | Spezifiziert das Gerät, das mit der Dateisystemressource verknüpft ist. Dabei kann es sich um ein Blockgerät, ein Dateisystem-Label, oder eine UUID eines Dateisystems handeln. |
| Options | Einhängeoptionen; also Optionen, die beim Einhängen des Dateisystems angewendet werden. Diese können dateisystemspezifisch sein. Siehe <code>mount(8)</code> Handbuchseite für die unterstützten Einhängeoptionen. |
| File System ID | <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;">  Anmerkung <i>File System ID</i> wird nur von NFS-Diensten verwendet. </div> <p>Beim Erstellen einer neuen Dateisystemressource können Sie dieses Feld leer lassen. Wenn Sie dieses Feld leer lassen, wird automatisch eine Dateisystem-ID zugewiesen, nachdem Sie den Parameter während der Konfiguration übergeben. Wenn Sie explizit eine Dateisystem-ID zuweisen müssen, geben Sie den gewünschten Wert in diesem Feld an.</p> |
| Force unmount | Falls aktiviert, wird das Dateisystem zum Aushängen gezwungen. Die Standardeinstellung ist disabled . Force Unmount würgt dabei sämtliche Prozesse ab, die den Einhängepunkt verwenden, damit das eingehängte Dateisystem beim Aushängen nicht mehr verwendet wird. |
| Reboot host node if unmount fails | Falls aktiviert, wird der Knoten, falls das Aushängen des Dateisystems fehlschlägt, neu gestartet. Die Standardeinstellung ist disabled . |
| Check file system before mounting | Falls aktiviert, wird <code>fsck</code> auf dem Dateisystem ausgeführt, bevor es eingehängt wird. Die Standardeinstellung ist disabled . |

Tabelle B.4. GFS2


| Feld | Beschreibung |
|--|---|
| Name | Der Name der Dateisystemressource. |
| Mount Point | Der Pfad, unter dem diese Dateisystemressource eingehängt wird. |
| Device | Die Gerätedatei, die mit der Dateisystemressource verknüpft ist. |
| Options | Einhängeoptionen. |
| File System ID | <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;">  Anmerkung <i>File System ID</i> wird nur von NFS-Diensten verwendet. </div> <p>Beim Erstellen einer neuen GFS2-Ressource können Sie dieses Feld leer lassen. Wenn Sie dieses Feld leer lassen, wird automatisch eine Dateisystem-ID zugewiesen, nachdem Sie den Parameter während der Konfiguration übergeben. Wenn Sie explizit eine Dateisystem-ID zuweisen müssen, geben Sie den gewünschten Wert in diesem Feld an.</p> |
| Force Unmount | Falls aktiviert, wird das Dateisystem zum Aushängen gezwungen. Die Standardeinstellung ist disabled . Force Unmount würgt dabei sämtliche Prozesse ab, die den Einhängepunkt verwenden, damit das eingehängte Dateisystem beim Aushängen nicht mehr verwendet wird. Bei GFS2-Ressourcen wird der Einhängepunkt beim Beenden eines Dienstes <i>nicht</i> ausgehängt, es sei denn, der Force Unmount ist <i>enabled</i> . |
| Reboot Host Node if Unmount Fails (self fence) | Falls aktiviert und falls das Aushängen des Dateisystems fehlschlägt, wird der Knoten sofort neu gestartet. Üblicherweise wird dies zusammen mit force-unmount-Unterstützung verwendet, dies ist jedoch nicht zwingend erforderlich. |

Tabelle B.5. IP-Adresse

| Feld | Beschreibung |
|--------------|--|
| IP-Adresse | Die IP-Adresse für die Ressource. Dies ist eine virtuelle IP-Adresse. IPv4 und IPv6 Adressen werden unterstützt, sowie NIC-Link-Überwachung für jede IP-Adresse. |
| Monitor Link | Ist dies aktiviert, schlägt die Statusüberprüfung fehl, falls der Link auf der NIC, an die diese IP-Adresse gebunden ist, nicht vorhanden ist. |

Tabelle B.6. LVM

| Feld | Beschreibung |
|--------------------------------|--|
| Name | Ein eindeutiger Name für diese LVM-Ressource. |
| Volume Group Name | Ein beschreibender Name der verwalteten Datenträgergruppe. |
| Logical Volume Name (optional) | Name des verwalteten logischen Datenträgers. Dieser Parameter ist optional, falls es mehr als einen logischen Datenträger in der verwalteten Datenträgergruppe gibt. |

Tabelle B.7. MySQL®

| Feld | Beschreibung |
|-------------------------|---|
| Name | Spezifiziert einen Namen für die MySQL-Serverressource. |
| Config File | Spezifiziert die Konfigurationsdatei. Der Standardwert ist <code>/etc/my.cnf</code> . |
| Listen Address | Spezifiziert eine IP-Adresse für MySQL-Server. Wird keine IP-Adresse angegeben, wird die erste IP-Adresse des Dienstes verwendet. |
| mysqld Options | Weitere Befehlszeilenoptionen für <code>httpd</code> . |
| Shutdown Wait (seconds) | Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird. |

Tabelle B.8. NFS Client

| Feld | Beschreibung |
|--------|--|
| Name | Dies ist ein symbolischer Name für einen Client, der zur Referenzierung im Ressourcenbaum verwendet wird. Dies ist <i>nicht</i> dasselbe wie die Target -Option. |
| Target | Dies ist der Server, von dem Sie einhängen. Er kann mittels Hostname, Platzhalter (basierend auf IP-Adresse oder Hostname) oder einer Netzgruppe spezifiziert werden, um Hosts zu definieren, auf die exportiert wird. |
| Option | Definiert eine Liste von Optionen für diesen Client — z.B. zusätzliche Client-Zugriffsrechte. Für weitere Informationen siehe exports (5) -Handbuchseite, <i>General Options</i> . |

Tabelle B.9. NFS Export


| Feld | Beschreibung |
|--|---|
| Name | Beschreibender Name der Ressource. Die NFS-Export-Ressource gewährleistet, dass NFS-Daemons laufen. Sie ist voll wiederverwendbar; normalerweise ist nur eine NFS-Export-Ressource nötig. |
|  Tip Benennen Sie die NFS-Export-Ressource so, dass sie deutlich von anderen NFS-Ressourcen zu unterscheiden ist. | |

Tabelle B.10. NFS/CIFS Mount


| Feld | Beschreibung |
|-------------------------------|--|
| Name | Symbolischer Name für den NFS oder CIFS Mount. |
| |  Anmerkung Diese Ressource ist nur dann nötig, wenn ein Cluster-Dienst als NFS-Client konfiguriert wird. |
| Mount Point | Der Pfad, unter dem diese Dateisystemressource eingehängt wird. |
| Host | IP-Adresse oder Hostname des NFS/CIFS-Servers. |
| NFS Export Path or CIFS share | Name des NFS-Export-Verzeichnisses oder CIFS-Shares. |
| File System type | Dateisystemtyp: <ul style="list-style-type: none"> ▶ NFS — Spezifiziert die Verwendung der standardmäßigen NFS-Version. Dies ist die Standardeinstellung. ▶ NFS v4 — Spezifiziert die Verwendung des NFSv4-Protokolls. ▶ CIFS — Spezifiziert die Verwendung des CIFS-Protokolls. |
| Options | Einhängeoptionen. Spezifiziert eine Liste mit Einhängeoptionen. Werden keine angegeben, wird das Dateisystem mit -o sync eingehängt. |
| Force Unmount | Falls Force Unmount aktiviert ist, würgt der Cluster beim Stoppen des Dienstes sämtliche Prozesse ab, die den Einhängepunkt verwenden, damit das eingehängte Dateisystem beim Aushängen nicht mehr verwendet wird. Andernfalls würde das Aushängen fehlschlagen und der Dienst würde neu gestartet werden. |
| No Unmount | Falls aktiviert, wird das Dateisystem während einer Stopp- oder Verlegungsoperation nicht ausgehängt. |

Tabelle B.11. Open LDAP

| Feld | Beschreibung |
|-------------------------|---|
| Name | Spezifiziert einen Dienstenamen zur Protokollierung und zu anderen Zwecken. |
| Config File | Spezifiziert einen absoluten Pfad zu einer Konfigurationsdatei. Der Standardwert lautet /etc/openldap/slapd.conf . |
| URL List | Der Standardwert ist ldap:/// . |
| slapd Options | Weitere Befehlszeilenoptionen für slapd . |
| Shutdown Wait (seconds) | Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird. |

Tabelle B.12. Oracle® 10g

| Feld | Beschreibung |
|--|---|
| Instance name (SID) of Oracle instance | Instanzname. |
| Oracle user name | Dies ist der Benutzername des Oracle-Benutzers, in dessen Namen die Oracle AS Instanz ausgeführt wird. |
| Oracle application home directory | Dies ist das Benutzerverzeichnis von Oracle (der Applikation, nicht des Benutzers). Es wird bei der Installation von Oracle konfiguriert. |
| Virtual hostname (optional) | Der virtuelle Hostname, der dem Installations-Hostnamen von Oracle 10g entspricht. Beachten Sie, dass Ihr Hostname beim Start/Stop einer oracledb-Ressource vorübergehend auf diesen Hostnamen geändert wird. Deshalb sollten Sie eine oracledb-Ressource nur als Teil eines exklusiven Dienstes konfigurieren. |

Tabelle B.13. PostgreSQL 8

| Feld | Beschreibung |
|-------------------------|--|
| Name | Spezifiziert einen Dienstenamen zur Protokollierung und zu anderen Zwecken. |
| Config File | Definiert einen absoluten Pfad zur Konfigurationsdatei. Der Standardwert lautet <code>/var/lib/pgsql/data/postgresql.conf</code> . |
| Postmaster User | Benutzer, der den Datenbank-Server ausführt, da dieser nicht von Root ausgeführt werden kann. Der Standardwert ist <code>postgres</code> . |
| Postmaster Options | Weitere Befehlszeilenoptionen für Postmaster. |
| Shutdown Wait (seconds) | Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird. |

Tabelle B.14. SAP®-Datenbank

| Feld | Beschreibung |
|---|--|
| SAP Database Name | Spezifiziert eine eindeutige SAP-Systemkennung, z.B. <code>P01</code> . |
| SAP executable directory | Spezifiziert den voll qualifizierten Pfad zu <code>sapstartsrv</code> und <code>sapcontrol</code> . |
| Database type | Spezifiziert eine der folgenden Datenbanktypen: Oracle, DB6 oder ADA. |
| Oracle TNS listener name | Spezifiziert den Oracle TNS Listener-Name. |
| ABAP stack is not installed, only Java stack is installed | Falls Sie keinen ABAP-Stapel in der SAP-Datenbank installiert haben, aktivieren Sie diesen Parameter. |
| J2EE instance bootstrap directory | Der voll qualifizierte Pfad des Bootstrap-Verzeichnisses der J2EE-Instanz, z.B. <code>/usr/sap/P01/J00/j2ee/cluster/bootstrap</code> . |
| J2EE security store path | Der voll qualifizierte Pfad des J2EE-Sicherheitspeicher-Verzeichnisses, z.B. <code>/usr/sap/P01/SYS/global/security/lib/tools</code> . |

Tabelle B.15. SAP®-Instanz

| Feld | Beschreibung |
|--|--|
| SAP Instance Name | Der vollqualifizierte Name der SAP-Instanz, z.B. P01_DVEBMGS00_sapp01ci. |
| SAP executable directory | Der vollqualifizierte Pfad zu sapstartsrv und sapcontrol . |
| Directory containing the SAP START profile | Der vollqualifizierte Pfad zum SAP START Profil. |
| Name of the SAP START profile | Spezifiziert den Namen des SAP START Profils. |

**Anmerkung**

Hinsichtlich [Tabelle B.16. „Samba-Dienst“](#) sei erwähnt, dass Sie beim Erstellen oder Ändern eines Cluster-Dienstes eine Samba-Dienstressource direkt mit dem Dienst verbinden sollten, *nicht* mit einer Ressource innerhalb eines Dienstes.

Tabelle B.16. Samba-Dienst

| Feld | Beschreibung |
|------|---|
| Name | Spezifiziert den Namen des Samba-Servers. |

Tabelle B.17. Skript

| Feld | Beschreibung |
|------------------|---|
| Name | Spezifiziert einen Namen für das angepasste Benutzerskript. Die Skriptressource ermöglicht es Ihnen, für den Start eines geclusterten Dienstes ein standardmäßiges, LSB-konformes init-Skript zu verwenden. |
| File (with path) | Geben Sie den Pfad an, auf dem sich dieses angepasste Skript befindet (z.B. /etc/init.d/userscript). |

Tabelle B.18. Dienst

| Feld | Beschreibung |
|----------------------------------|---|
| Service name | Name des Dienstes. Dies definiert eine Sammlung von Ressourcen, auch Ressourcengruppe oder Cluster-Dienst genannt. |
| Automatically start this service | Falls aktiviert, wird dieser Dienst (oder diese Ressourcengruppe) automatisch gestartet, sobald der Cluster ein Quorum bildet. Ist dieser Parameter <i>disabled</i> , startet dieser Dienst <i>nicht</i> automatisch, sobald der Cluster ein Quorum bildet; der Dienst wird in den disabled -Status versetzt. |
| Run exclusive | Falls aktiviert, kann dieser Dienst (oder diese Ressourcengruppe) nur verlegt werden, wenn er auf dem anderen Knoten exklusiv läuft; er kann also nur auf einen Knoten verlegt werden, auf dem keine anderen Dienste ausgeführt werden. Falls keine Knoten zur Verfügung stehen, die einen Dienst exklusiv ausführen könnten, wird dieser Dienst nach einem Ausfall nicht wieder gestartet. Außerdem werden andere Dienste nicht automatisch auf einen Knoten verlegt, der diesen Dienst als Run exclusive ausführt. Sie können diese Option mithilfe manueller Start- oder Relocate-Operationen außer Kraft setzen. |
| Failover Domain | Definiert eine Liste mit Cluster-Mitgliedern, die im Falle eines Dienstausfalls ersatzweise versucht werden sollen. |
| Recovery policy | Recovery policy bietet die folgenden Optionen: <ul style="list-style-type: none"> ▶ Disable — Deaktiviert die Ressourcengruppe, falls eine der Komponenten ausfällt. ▶ Relocate — Versucht, den Dienst auf einem anderen Knoten zu starten, anstatt zu versuchen, den Dienst auf dem derzeitigen Knoten neu zu starten. ▶ Restart — Versucht, fehlgeschlagene Teile dieses Dienstes lokal (auf dem derzeitigen Knoten) neu zu starten, bevor versucht wird, den Dienst auf einen anderen Knoten zu verlegen (Standard). ▶ Restart-Disable — Der Dienst wird nach einem Ausfall an derselben Stelle neu gestartet. Falls der Neustart jedoch fehlschlägt, wird der Dienst nicht auf einen anderen Host im Cluster verlegt, sondern deaktiviert. |

Tabelle B.19. Sybase® ASE-Ausfallsicherungsinstanz


| Feld | Beschreibung |
|---------------------------|---|
| Instance Name | Spezifiziert den Instanzennamen der Sybase ASE-Ressource. |
| ASE server name | Der ASE-Servername, der für den Hochverfügbarkeitsdienst konfiguriert ist. |
| Sybase home directory | Das Benutzerverzeichnis für Sybase-Produkte. |
| Login file | Der vollständige Pfad zur Login-Datei, die das Login-Passwort-Paar enthält. |
| Interfaces file | Der vollständige Pfad zur Schnittstellendatei, die zum Starten und zum Zugriff auf den ASE-Server verwendet wird. |
| SYBASE_ASE directory name | Der Verzeichnisname unter sybase_home, wo ASE-Produkte installiert werden. |
| SYBASE_OCS directory name | Der Verzeichnisname unter sybase_home, wo OCS-Produkte installiert werden, z.B. ASE-15_0. |
| Sybase user | Der Benutzer, der den ASE-Server ausführen kann. |
| Deep probe timeout | Die maximale Anzahl von Sekunden, die auf eine Antwort vom ASE-Server gewartet wird, bevor davon ausgegangen wird, dass der Server während der Deep-Probe keine Antwort erhalten hat. |

Tabelle B.20. Tomcat 6

| Feld | Beschreibung |
|-------------------------|---|
| Name | Spezifiziert einen Dienstnamen zur Protokollierung und zu anderen Zwecken. |
| Config File | Spezifiziert den absoluten Pfad zu einer Konfigurationsdatei. Der Standardwert lautet /etc/tomcat6/tomcat6.conf . |
| Tomcat User | Benutzer, der den Tomcat-Server ausführt. Der Standardwert ist <i>tomcat</i> . |
| Catalina Options | Weitere Befehlszeilenoptionen für Catalina. |
| Catalina Base | Catalina-Basisverzeichnis (für jeden Dienst unterschiedlich). Der Standardwert ist <i>/usr/share/tomcat6</i> . |
| Shutdown Wait (seconds) | Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird. Der Standardwert ist 30. |

Tabelle B.21. Virtuelle Maschine

| Feld | Beschreibung |
|--|---|
| Name | Spezifiziert den Namen der virtuellen Maschine. Wenn Sie die Luci -Oberfläche verwenden, spezifizieren Sie dies als Dienstnamen. |
| Automatically start this virtual machine | Falls aktiviert, wird diese virtuelle Maschine automatisch gestartet, sobald der Cluster ein Quorum bildet. Ist dieser Parameter <i>disabled</i> , startet diese virtuelle Maschine <i>nicht</i> automatisch, sobald der Cluster ein Quorum bildet; die virtuelle Maschine wird in den disabled -Status versetzt. |
| Run exclusive | Falls aktiviert, kann diese virtuelle Maschine nur verlegt werden, wenn sie auf dem anderen Knoten exklusiv läuft; sie kann also nur auf einen Knoten verlegt werden, auf dem keine anderen virtuellen Maschinen ausgeführt werden. Falls keine Knoten zur Verfügung stehen, die eine virtuelle Maschine exklusiv ausführen könnten, wird diese virtuelle Maschine nach einem Ausfall nicht wieder gestartet. Außerdem werden andere virtuelle Maschinen nicht automatisch auf einen Knoten verlegt, der diese virtuelle Maschine als Run exclusive ausführt. Sie können diese Option mithilfe manueller Start- oder Relocate-Operationen außer Kraft setzen. |
| Failover domain | Definiert eine Liste mit Cluster-Mitgliedern, die im Falle eines Ausfalls der virtuellen Maschine ersatzweise versucht werden sollen. |
| Recovery policy | Recovery policy bietet die folgenden Optionen: <ul style="list-style-type: none"> ▶ Disable — Deaktiviert die virtuelle Maschine, falls diese ausfällt. ▶ Relocate — Versucht, die virtuelle Maschine auf einem anderen Knoten zu starten, anstatt zu versuchen, sie auf dem derzeitigen Knoten neu zu starten. ▶ Restart — Versucht, die virtuelle Maschine lokal (auf dem derzeitigen Knoten) neu zu starten, bevor versucht wird, sie auf einen anderen Knoten zu verlegen (Standard). ▶ Restart-Disable — Der Dienst wird nach einem Ausfall an derselben Stelle neu gestartet. Falls der Neustart jedoch fehlschlägt, wird der Dienst nicht auf einen anderen Host im Cluster verlegt, sondern deaktiviert. |
| Restart options | Falls Sie Restart oder Restart-Disable als Wiederherstellungsrichtlinie für einen Dienst auswählen, können Sie die maximale Anzahl an Neustartfehlschlägen festlegen, bevor der Dienst verlegt oder deaktiviert wird, sowie die Zeitspanne in Sekunden, nach der ein Neustart nicht weiter versucht werden soll. |
| Migration type | Spezifiziert den Migrationstyp live oder pause . Die Standardeinstellung ist live . |
| Migration mapping | Spezifiziert eine alternative Schnittstelle für die Migration. Sie können dies beispielsweise festlegen, wenn sich die Netzwerkadresse für die Migration der virtuellen Maschine eines Knotens von der Adresse des Knotens für die Cluster-Kommunikation unterscheidet. Folgende Angaben führen dazu, dass Sie beim Migrieren einer virtuellen Maschine von member nach member2 tatsächlich nach target2 migrieren. Wenn Sie von member2 nach member migrieren, wird target zur Migration verwendet. member : target , member2 : target2 |
| Status Program | Das auszuführende Statusprogramm, zusätzlich zur standardmäßigen Überprüfung auf virtuelle Maschinen hin. Falls spezifiziert, wird das Statusprogramm einmal pro Minute ausgeführt. Dies erlaubt Ihnen, den Status kritischer Dienste innerhalb einer virtuellen Maschine zu bestimmen. Wenn Ihre virtuelle Maschine beispielsweise einen Webserver ausführt, sollte Ihr Statusprogramm überprüfen, ob ein Webserver läuft; falls die Statusüberprüfung fehlschlägt (gekennzeichnet durch eine nicht-Null Ausgabe), wird die virtuelle Maschine wiederhergestellt. Nachdem eine virtuelle Maschine gestartet wurde, wird der Ressourcen-Agent der virtuellen Maschine regelmäßig das Statusprogramm ausführen und auf einen erfolgreichen Antwort-Code (Null) warten, bevor er zurückkehrt. Nach fünf Minuten erfolgt eine Zeitüberschreitung. |

| | |
|---|--|
| Path to XML file used to create the VM | Vollständiger Pfad zur libvirt XML-Datei, welche die libvirt -Domain-Definition enthält. |
| VM configuration file path | Eine durch Doppelpunkt getrennte Pfadspezifikation, die der Ressourcen-Agent der virtuellen Maschine (vm.sh) nach der Konfigurationsdatei der virtuellen Maschine durchsucht. Zum Beispiel: /mnt/guests/config:/etc/libvirt/qemu . |
|  Wichtig | |
| Der Pfad sollte <i>nie</i> direkt auf eine Konfigurationsdatei einer virtuellen Maschine verweisen. | |
| Path to VM snapshot directory | Pfad zum Snapshot-Verzeichnis, in dem das virtuelle Maschinen-Image gespeichert wird. |
| Hypervisor URI | Hypervisor-URI (normalerweise automatisch). |
| Migration URI | Migrations-URI (normalerweise automatisch). |

Verhalten der Hochverfügbarkeitsressourcen

Dieser Anhang beschreibt das übliche Verhalten von Hochverfügbarkeitsressourcen. Es soll Ihnen ergänzende Informationen liefern, die Ihnen bei der Konfiguration von Hochverfügbarkeitsdiensten helfen können. Sie können die Parameter mithilfe von **Luci** konfigurieren, oder indem Sie **etc/cluster/cluster.conf** bearbeiten. Beschreibungen der Parameter der Hochverfügbarkeitsressourcen finden Sie in [Anhang B, Parameter der Hochverfügbarkeitsressourcen](#). Für ein besseres Verständnis von Ressourcen-Agents können Sie sich diese in **/usr/share/cluster** in jedem beliebigen Cluster-Knoten ansehen.



Anmerkung

Um die Informationen in diesem Anhang umfassend verstehen zu können, benötigen Sie u.U. ebenfalls ein umfassendes Verständnis der Ressourcen-Agents und der Cluster-Konfigurationsdatei **/etc/cluster/cluster.conf**.

Ein Hochverfügbarkeitsdienst besteht aus einer Gruppe von Cluster-Ressourcen, die als eine zusammenhängende Einheit konfiguriert wurden und zusammen einen spezialisierten Dienst für Clients bereitstellen. Ein Hochverfügbarkeitsdienst wird als Ressourcenbaum in der Cluster-Konfigurationsdatei **/etc/cluster/cluster.conf** dargestellt (in jedem Cluster-Knoten). In der Cluster-Konfigurationsdatei ist jeder Ressourcenbaum eine XML-Darstellung, die jede Ressource spezifiziert, deren Parameter, sowie ihre Relationen zu anderen Ressourcen im Ressourcenbaum (Eltern-, Kind-, Geschwisterrelationen).



Anmerkung

Da ein Hochverfügbarkeitsdienst aus Ressourcen besteht, die in einem hierarchischen Baum angeordnet sind, wird ein solcher Dienst manchmal auch als *Ressourcenbaum* oder *Ressourcengruppe* bezeichnet. Beide Ausdrücke sind Synonyme für *Hochverfügbarkeitsdienst*.

An der Wurzel (Root) eines jeden Ressourcenbaums befindet sich eine besondere Art von Ressource — eine *Dienstressource*. Andere Arten von Ressourcen bilden den Rest eines Dienstes und bestimmen so dessen Charakteristiken. Zum Erstellen eines Hochverfügbarkeitsdienstes gehört das Erstellen einer Dienstressource, das Erstellen untergeordneter Cluster-Ressourcen, sowie deren Anordnung in eine zusammenhängende Einheit gemäß den hierarchischen Einschränkungen des Dienstes.

Dieser Anhang umfasst die folgenden Abschnitte:

- ▶ [Abschnitt C.1, „Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen“](#)
- ▶ [Abschnitt C.2, „Startreihenfolge von Kind- und Geschwisterressourcen“](#)
- ▶ [Abschnitt C.3, „Vererbung, der <resources>-Block, und Wiederverwendung von Ressourcen“](#)
- ▶ [Abschnitt C.4, „Wiederherstellung nach Ausfall und Unabhängige Unterbäume“](#)
- ▶ [Abschnitt C.5, „Testen und Fehlerbehebung von Diensten und der Ressourcenreihenfolge“](#)



Anmerkung

Die folgenden Abschnitte zeigen Beispiele der Cluster-Konfigurationsdatei **/etc/cluster/cluster.conf**, die jedoch nur der Veranschaulichung dienen sollen.

C.1. Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen

Ein Cluster-Dienst ist eine integrierte Einheit, die unter der Kontrolle von **rgmanager** läuft. Alle Ressourcen in einem Dienst laufen auf demselben Knoten. Aus Sicht des **rgmanager** ist ein Cluster-

Dienst eine Einheit, die gestartet, gestoppt oder verlegt werden kann. Innerhalb eines Cluster-Dienstes bestimmt jedoch die Hierarchie der Ressourcen, in welcher Reihenfolge die Ressourcen gestartet und gestoppt werden. Die Hierarchieebenen sind Eltern, Kinder und Geschwister.

[Beispiel C.1, „Ressourcenhierarchie des Dienstes foo“](#) zeigt ein Beispiel für einen Ressourcenbaum des Dienstes *foo*. In diesem Beispiel stehen die Ressourcen wie folgt miteinander in Relation:

- ▶ **fs:myfs** (<fs name="myfs" ...>) und **ip:10.1.1.2** (<ip address="10.1.1.2 .../>) sind Geschwister.
- ▶ **fs:myfs** (<fs name="myfs" ...>) sind die Eltern von **script:script_child** (<script name="script_child"/>).
- ▶ **script:script_child** (<script name="script_child"/>) ist das Kind von **fs:myfs** (<fs name="myfs" ...>).

Beispiel C.1. Ressourcenhierarchie des Dienstes foo

```
<service name="foo" ...>
  <fs name="myfs" ...>
    <script name="script_child"/>
  </fs>
  <ip address="10.1.1.2" .../>
</service>
```

Die folgenden Regeln gelten für Eltern/Kind-Relationen in einem Ressourcenbaum:

- ▶ Eltern werden vor ihren Kindern gestartet.
- ▶ Kinder müssen alle sauber gestoppt worden sein, bevor die Eltern gestoppt werden dürfen.
- ▶ Damit eine Ressource als "gesund" betrachtet wird, müssen alle ihre Kinder ebenfalls "gesund" sein.

C.2. Startreihenfolge von Kind- und Geschwisterressourcen

Die Dienstressource bestimmt die Start- und Stoppreihenfolge einer Kindressource danach, ob diese ein Kind-Typ-Parameter für eine Kindressource kennzeichnet, und zwar wie folgt:

- ▶ Gekennzeichnet mit dem Kind-Typ-Parameter (*typisiert* als Kindressource) — Falls die Dienstressource eine Kindressource mit dem Kind-Typ-Parameter kennzeichnet, ist die Kindressource *typisiert*. Der Kind-Typ-Parameter bestimmt explizit die Start- und Stoppreihenfolge der Kindressource.
- ▶ *Nicht gekennzeichnet* mit dem Kind-Typ-Parameter (*nicht typisiert* als Kindressource) — Falls die Dienstressource eine Kindressource *nicht* mit dem Kind-Typ-Parameter kennzeichnet, ist die Kindressource *nicht typisiert*. Die Dienstressource steuert nicht explizit die Start- und Stoppreihenfolge einer nicht typisierten Kindressource. Allerdings wird eine nicht typisierte Kindressource gemäß der Reihenfolge in `/etc/cluster.cluster.conf` gestartet und gestoppt. Zudem werden nicht typisierte Kindressourcen gestartet, nachdem alle typisierten Kindressourcen gestartet wurden, und sie werden gestoppt, bevor jegliche typisierten Kindressourcen gestoppt werden.



Anmerkung

Die einzige Ressource, die eine Sortierung nach definierten *Kind-Ressourcentyp* implementiert, ist die Dienstressource.

Weitere Informationen über die Start-/Stopp-Reihenfolge von typisierten Kindressourcen finden Sie in [Abschnitt C.2.1, „Start-/Stopp-Reihenfolge von typisierten Kindressourcen“](#). Weitere Informationen über die Start-/Stopp-Reihenfolge von nicht typisierten Kindressourcen finden Sie in [Abschnitt C.2.2, „Start-](#)

[und Stoppreihenfolge von nicht typisierten Kindressourcen“.](#)

C.2.1. Start-/Stopp-Reihenfolge von typisierten Kindressourcen

Bei einer typisierten Kindressource definiert der Typparameter der Kindressource die Start- und Stoppreihenfolge eines jeden Ressourcentyps mit einer Nummer von 1 bis 100; ein Wert für den Start, und ein Wert für den Stopp. Je niedriger die Nummer, desto früher wird ein Ressourcentyp gestartet oder gestoppt. [Tabelle C.1, „Start-/Stopp-Reihenfolge von typisierten Kindressourcen“](#) zeigt beispielsweise die Start- und Stoppwerte für jeden Ressourcentyp; [Beispiel C.2, „Start und Stopp-Werte der Ressourcen: Auszug aus dem Dienstressourcen-Agent, `service.sh`“](#) zeigt die Start- und Stoppwerte, wie sie im Dienstressourcen-Agent, `service.sh`, erscheinen. Für die Dienstressource werden alle LVM-Kinder zuerst gestartet, gefolgt von allen Dateisystem-Kindern, wiederum gefolgt von allen Skript-Kindern, usw.

Tabelle C.1. Start-/Stopp-Reihenfolge von typisierten Kindressourcen

| Ressource | Kindtyp | Startreihenfolge | Stoppreihenfolge |
|------------------|-----------|------------------|------------------|
| LVM | lvm | 1 | 9 |
| Dateisystem | fs | 2 | 8 |
| GFS2-Dateisystem | clusterfs | 3 | 7 |
| NFS Mount | netfs | 4 | 6 |
| NFS Export | nfsexport | 5 | 5 |
| NFS Client | nfsclient | 6 | 4 |
| IP-Adresse | ip | 7 | 2 |
| Samba | smb | 8 | 3 |
| Skript | script | 9 | 1 |

Beispiel C.2. Start und Stopp-Werte der Ressourcen: Auszug aus dem Dienstressourcen-Agent, `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>
```

Die Reihenfolge innerhalb eines Ressourcentyps wird bewahrt, da sie in der Cluster-Konfigurationsdatei `/etc/cluster/cluster.conf` gespeichert wird. Sehen Sie sich zum Beispiel die Start- und Stoppreihenfolge der typisierten Kindressourcen in [Beispiel C.3, „Reihenfolge innerhalb eines Ressourcentyps“](#) an.

Beispiel C.3. Reihenfolge innerhalb eines Ressourcentyps

```
<service name="foo">
  <script name="1" .../>
  <lvm name="1" .../>
  <ip address="10.1.1.1" .../>
  <fs name="1" .../>
  <lvm name="2" .../>
</service>
```

Startreihenfolge von typisierten Kindressourcen

In [Beispiel C.3. „Reihenfolge innerhalb eines Ressourcentyps“](#) werden die Ressourcen in der folgenden Reihenfolge gestartet:

1. **lvm:1** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuerst gestartet. **lvm:1** (`<lvm name="1" .../>`) ist die erste LVM-Ressource, die von allen LVM-Ressourcen als erste gestartet wird, da dies die erste LVM-Ressource ist, die im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt wird.
2. **lvm:2** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuerst gestartet. **lvm:2** (`<lvm name="2" .../>`) wird nach **lvm:1** gestartet, da sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` nach **lvm:1** aufgeführt wird.
3. **fs:1** — Dies ist eine Dateisystemressource. Gäbe es noch weitere Dateisystemressourcen im Dienst *foo*, so starteten diese in der Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
4. **ip:10.1.1.1** — Dies ist eine IP-Adress-Ressource. Gäbe es noch weitere IP-Adress-Ressourcen im Dienst *foo*, so starteten diese in der Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
5. **script:1** — Dies ist eine Skriptressource. Gäbe es noch weitere Skriptressourcen im Dienst *foo*, so starteten diese in der Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.

Stoppreihenfolge von typisierten Kindressourcen

In [Beispiel C.3. „Reihenfolge innerhalb eines Ressourcentyps“](#) werden die Ressourcen in der folgenden Reihenfolge gestoppt:

1. **script:1** — Dies ist eine Skriptressource. Gäbe es noch weitere Skriptressourcen im Dienst *foo*, so stoppten diese in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
2. **ip:10.1.1.1** — Dies ist eine IP-Adress-Ressource. Gäbe es noch weitere IP-Adress-Ressourcen im Dienst *foo*, so stoppten diese in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
3. **fs:1** — Dies ist eine Dateisystemressource. Gäbe es noch weitere Dateisystemressourcen im *foo*, so stoppten diese in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
4. **lvm:2** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuletzt gestoppt. **lvm:2** (`<lvm name="2" .../>`) wird vor **lvm:1** gestoppt; Ressourcen innerhalb einer Ressourcentyp-Gruppe werden in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden, gestoppt.
5. **lvm:1** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuletzt gestoppt. **lvm:1** (`<lvm name="1" .../>`) wird nach **lvm:2** gestoppt; Ressourcen innerhalb einer Ressourcentyp-Gruppe werden in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden, gestoppt.

C.2.2. Start- und Stoppreihenfolge von nicht typisierten Kindressourcen

Für nicht typisierte Kindressourcen sind zusätzliche Überlegungen notwendig. Bei einer nicht typisierten Kindressource wird die Start- und Stoppreihenfolge nicht explizit durch die Dienstressource spezifiziert. Stattdessen wird die Start- und Stoppreihenfolge abhängig von der Reihenfolge der Kindressourcen in `/etc/cluster.cluster.conf` bestimmt. Zudem werden nicht typisierte Kindressourcen erst nach allen typisierten Kindressourcen gestartet, und bevor jeglichen typisierten Kindressourcen gestoppt.

Sehen Sie sich zum Beispiel die Start- und Stoppreihenfolge der nicht typisierten Kindressourcen in [Beispiel C.4, „Nicht typisierte und typisierte Kindressource in einem Dienst“](#) an.

Beispiel C.4. Nicht typisierte und typisierte Kindressource in einem Dienst

```
<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>
```

Startreihenfolge von nicht typisierten Kindressourcen

In [Beispiel C.4, „Nicht typisierte und typisierte Kindressource in einem Dienst“](#) werden die Kindressourcen in der folgenden Reihenfolge gestartet:

1. **lvm:1** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuerst gestartet. **lvm:1** (`<lvm name="1" .../>`) ist die erste LVM-Ressource, die von allen LVM-Ressourcen als erste gestartet wird, da dies die erste LVM-Ressource ist, die im `foo`-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt wird.
2. **lvm:2** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuerst gestartet. **lvm:2** (`<lvm name="2" .../>`) wird nach **lvm:1** gestartet, da sie im `foo`-Dienstabschnitt von `/etc/cluster/cluster.conf` nach **lvm:1** aufgeführt wird.
3. **fs:1** — Dies ist eine Dateisystemressource. Gäbe es noch weitere Dateisystemressourcen im Dienst `foo`, so starteten diese in der Reihenfolge, in der Sie im `foo`-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
4. **ip:10.1.1.1** — Dies ist eine IP-Adress-Ressource. Gäbe es noch weitere IP-Adress-Ressourcen im Dienst `foo`, so starteten diese in der Reihenfolge, in der Sie im `foo`-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
5. **script:1** — Dies ist eine Skriptressource. Gäbe es noch weitere Skriptressourcen im Dienst `foo`, so starteten diese in der Reihenfolge, in der Sie im `foo`-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
6. **nontypedresource:foo** — Dies ist eine nicht typisierte Ressource. Da es sich um eine nicht typisierte Ressource handelt, wird sie erst nach den typisierten Ressourcen gestartet. Zudem ist ihre Position in der Dienstressource vor der anderen nicht typisierten Ressource, **nontypedresourcetwo:bar**; daher wird sie noch vor **nontypedresourcetwo:bar** gestartet. (Nicht typisierte Ressourcen werden in der Reihenfolge gestartet, in der sie in der Dienstressource aufgeführt werden.)
7. **nontypedresourcetwo:bar** — Dies ist eine nicht typisierte Ressource. Da es sich um eine nicht typisierte Ressource handelt, wird sie erst nach den typisierten Ressourcen gestartet. Zudem ist ihre Position in der Dienstressource nach der anderen nicht typisierten Ressource, **nontypedresource:foo**; daher wird sie nach **nontypedresource:foo** gestartet. (Nicht typisierte Ressourcen werden in der Reihenfolge gestartet, in der sie in der Dienstressource aufgeführt werden.)

Stoppreihenfolge von nicht typisierten Kindressourcen

In [Beispiel C.4, „Nicht typisierte und typisierte Kindressource in einem Dienst“](#) werden die Kindressourcen in der folgenden Reihenfolge gestoppt:

1. **nontypedresourcetwo:bar** — Dies ist eine nicht typisierte Ressource. Da es sich um eine nicht typisierte Ressource handelt, wird sie vor den typisierten Ressourcen gestoppt. Zudem ist ihre Position in der Dienstressource nach der anderen nicht typisierten Ressource, **nontypedresource:foo**; daher wird sie vor **nontypedresource:foo** gestoppt. (Nicht typisierte Ressourcen werden in der umgekehrten Reihenfolge gestoppt, in der sie in der Dienstressource aufgeführt werden.)
2. **nontypedresource:foo** — Dies ist eine nicht typisierte Ressource. Da es sich um eine nicht typisierte Ressource handelt, wird sie vor den typisierten Ressourcen gestoppt. Zudem ist ihre Position in der Dienstressource vor der anderen nicht typisierten Ressource, **nontypedresourcetwo:bar**; daher wird sie nach **nontypedresourcetwo:bar** gestoppt. (Nicht typisierte Ressourcen werden in der umgekehrten Reihenfolge gestoppt, in der sie in der Dienstressource aufgeführt werden.)
3. **script:1** — Dies ist eine Skriptressource. Gäbe es noch weitere Skriptressourcen im Dienst *foo*, so stoppten diese in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
4. **ip:10.1.1.1** — Dies ist eine IP-Adress-Ressource. Gäbe es noch weitere IP-Adress-Ressourcen im Dienst *foo*, so stoppten diese in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
5. **fs:1** — Dies ist eine Dateisystemressource. Gäbe es noch weitere Dateisystemressourcen im *foo*, so stoppten diese in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden.
6. **lvm:2** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuletzt gestoppt. **lvm:2** (`<lvm name="2" .../>`) wird vor **lvm:1** gestoppt; Ressourcen innerhalb einer Ressourcentyp-Gruppe werden in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden, gestoppt.
7. **lvm:1** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuletzt gestoppt. **lvm:1** (`<lvm name="1" .../>`) wird nach **lvm:2** gestoppt; Ressourcen innerhalb einer Ressourcentyp-Gruppe werden in der umgekehrten Reihenfolge, in der Sie im *foo*-Dienstabschnitt von `/etc/cluster/cluster.conf` aufgeführt werden, gestoppt.

C.3. Vererbung, der <resources>-Block, und Wiederverwendung von Ressourcen

Einige Ressourcen können davon profitieren, Werte von einer Elternressource zu erben; dies ist zum Beispiel üblicherweise bei einem NFS-Dienst der Fall. [Beispiel C.5, „NFS-Dienst eingerichtet zur Ressourcenwiederverwendung und Vererbung“](#) zeigt eine typische NFS-Dienstkonfiguration, die zur Ressourcenwiederverwendung und Vererbung eingerichtet ist.

Beispiel C.5. NFS-Dienst eingerichtet zur Ressourcenwiederverwendung und Vererbung

```

<resources>
  <nfsclient name="bob" target="bob.test.com" options="rw,no_root_squash"/>
  <nfsclient name="jim" target="jim.test.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>

```

Wäre dieser Dienst flach (also ohne Eltern-/Kind-Relationen), müsste er wie folgt konfiguriert werden:

- ▶ Der Dienst benötigte vier `nfsclient`-Ressourcen — eine pro Dateisystem (insgesamt zwei für Dateisysteme), und eine pro Zielrechner (insgesamt zwei für Zielrechner).
- ▶ Der Dienst müsste den Exportpfad und die Dateisystem-ID für jeden `nfsclient` spezifizieren, was mögliche Fehlerquellen in die Konfiguration einbringt.

In [Beispiel C.5, „NFS-Dienst eingerichtet zur Ressourcenwiederverwendung und Vererbung“](#) werden die NFS-Client-Ressourcen `nfsclient:bob` und `nfsclient:jim` jedoch nur einmal definiert; ebenso wird die NFS-Export-Ressource `nfsexport:exports` nur einmal definiert. Alle von den Ressourcen benötigten Parameter werden von der Elternressource geerbt. Da die vererbten Parameter dynamisch sind (und nicht miteinander in Konflikt stehen), ist es möglich, diese Ressourcen wiederzuverwenden — weshalb sie im Ressourcenblock definiert sind. Es ist nicht sehr praktisch, manche Ressourcen an mehreren Stellen zu konfigurieren. Wenn Sie z.B. eine Dateisystemressource an mehreren Stellen konfigurieren, kann dies dazu führen, dass ein Dateisystem in zwei Knoten eingehängt wird und dadurch Probleme verursacht.

C.4. Wiederherstellung nach Ausfall und Unabhängige Unterbäume

In den meisten Unternehmensumgebungen wird zur Wiederherstellung nach einem Dienstausschlag in der Regel der gesamte Dienst neu gestartet, auch wenn nur Teilkomponenten des Dienstes ausgefallen waren. Wenn in [Beispiel C.6, „Dienst foo - Normale Wiederherstellung nach Ausfall“](#) z.B. eines der Skripte fehlschlägt, die in diesem Dienst definiert werden, so wird in der Regel der Dienst neu gestartet (oder verlegt oder deaktiviert, je nach Wiederherstellungsrichtlinie des Dienstes). In einigen Fällen

können bestimmte Teile eines Dienstes als nicht-kritisch betrachtet werden; es kann notwendig sein, den Dienst nur in Teilen neu zu starten, bevor die normale Wiederherstellungsprozedur begonnen wird. Sie können zu diesem Zweck den `__independent_subtree`-Parameter verwenden. In [Beispiel C.7, „Dienst foo - Wiederherstellung nach Ausfall mit `__independent_subtree`-Parameter“](#) wird der `__independent_subtree`-Parameter verwendet, um die folgenden Aktionen durchzuführen:

- ▶ Falls `script:script_one` fehlschlägt, werden `script:script_one`, `script:script_two` und `script:script_three` neu gestartet.
- ▶ Falls `script:script_two` fehlschlägt, wird nur `script:script_two` neu gestartet.
- ▶ Falls `script:script_three` fehlschlägt, werden `script:script_one`, `script:script_two` und `script:script_three` neu gestartet.
- ▶ Falls `script:script_four` fehlschlägt, wird der gesamte Dienst neu gestartet.

Beispiel C.6. Dienst foo - Normale Wiederherstellung nach Ausfall

```
<service name="foo">
  <script name="script_one" ...>
    <script name="script_two" .../>
  </script>
  <script name="script_three" .../>
</service>
```

Beispiel C.7. Dienst foo - Wiederherstellung nach Ausfall mit `__independent_subtree`-Parameter

```
<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>
```

Unter Umständen möchten Sie beim Ausfall einer Dienstkomponente nur diese einzelne Komponente deaktivieren, ohne den gesamten Dienst zu deaktivieren, damit andere Dienste, die andere Komponenten dieses Dienstes nutzen, nicht ebenfalls in Mitleidenschaft gezogen werden. Ab der Red Hat Enterprise Linux 6.1 Release können Sie zu diesem Zweck den `__independent_subtree="2"` Parameter nutzen, der den unabhängigen Unterbaum als nicht kritisch kennzeichnet.



Anmerkung

Sie können das nicht-kritisch Flag nur auf Ressourcen mit einer einzigen Referenz anwenden. Das nicht-kritisch Flag funktioniert mit allen Ressourcen auf allen Ebenen des Ressourcenbaums, sollte jedoch nicht auf oberster Ebene angewendet werden, wenn Dienste oder virtuelle Maschinen definiert werden.


Ab der Red Hat Enterprise Linux 6.1 Release können Sie die maximalen Neustarts und den Neustart-Ablauf pro Knoten für unabhängige Unterbäume im Ressourcenbaum angeben. Um diese Grenzwerte einzustellen, verwenden Sie die folgenden Parameter:

- ▶ `__max_restarts` konfiguriert die Höchstanzahl der geduldeten Neustarts, bevor abgebrochen wird.
- ▶ `__restart_expire_time` konfiguriert die Zeitspanne in Sekunden, nach der kein Neustart mehr versucht wird.

C.5. Testen und Fehlerbehebung von Diensten und der Ressourcenreihenfolge

Sie können mithilfe des `rg_test`-Dienstprogramms die Dienste und die Ressourcenreihenfolge testen und ggf. korrigieren. Bei `rg_test` handelt es sich um ein Befehlszeilen-Tool, das vom `rgmanager`-Paket bereitgestellt wird, und von einer Shell oder einem Terminal ausgeführt wird (es ist nicht in `Conga` verfügbar). [Tabelle C.2, „Übersicht über das `rg_test`-Dienstprogramm“](#) fasst die Aktionen und die Syntax für das `rg_test`-Dienstprogramm zusammen.

Tabelle C.2. Übersicht über das `rg_test`-Dienstprogramm

| Aktion | Syntax |
|---|---|
| Zeigt die Ressourcenregeln an, die <code>rg_test</code> versteht. | <code>rg_test rules</code> |
| Überprüft eine Konfiguration (und <code>/usr/share/cluster</code>) auf Fehler oder redundante Ressourcen-Agents. | <code>rg_test test /etc/cluster/cluster.conf</code> |
| Zeigt die Start- und Stoppreihenfolge eines Dienstes. | Anzeige der Startreihenfolge: <code>rg_test noop /etc/cluster/cluster.conf start service <i>servicename</i></code> Anzeige der Stoppreihenfolge: <code>rg_test noop /etc/cluster/cluster.conf stop service <i>servicename</i></code> |
| Startet oder stoppt einen Dienst explizit. | <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;">  Wichtig Führen Sie dies nur auf einem Knoten aus und deaktivieren Sie den Dienst vorher grundsätzlich in <code>rgmanager</code>. </div> Starten eines Dienstes: <code>rg_test test /etc/cluster/cluster.conf start service <i>servicename</i></code> Stoppen eines Dienstes: <code>rg_test test /etc/cluster/cluster.conf stop service <i>servicename</i></code> |
| Berechnet und zeigt das Ressourcenbaum-Delta zwischen zwei <code>cluster.conf</code> -Dateien. | <code>rg_test delta <i>cluster.conf file 1 cluster.conf file 2</i></code> Zum Beispiel: <code>rg_test delta /etc/cluster/cluster.conf.bak /etc/cluster/cluster.conf</code> |

Überblick über Befehlszeilen-Tools

[Tabelle D.1, „Überblick über Befehlszeilen-Tools“](#) fasst die bevorzugten Befehlszeilen-Tools zur Konfiguration und zur Verwaltung des Hochverfügbarkeits-Add-Ons zusammen. Werfen Sie für weitere Informationen über Befehle und Variablen bitte einen Blick auf die Handbuchseite des jeweiligen Befehlszeilen-Tools.

Tabelle D.1. Überblick über Befehlszeilen-Tools

| Befehlszeilen-Tool | Verwendet mit | Zweck |
|---|---|---|
| ccs_config_dump — Tool zum Speicherauszug der Cluster-Konfiguration | Cluster-Infrastruktur | ccs_config_dump generiert eine XML-Ausgabe der laufenden Konfiguration. Die laufende Konfiguration kann sich unter Umständen von der gespeicherten Konfiguration unterscheiden, da einige Untersysteme bestimmte Standardinformationen in der Konfiguration ablegen oder einstellen. Diese Werte sind in der Regel nicht in der auf der Festplatte gespeicherten Version der Konfiguration vorhanden, sind jedoch zur Laufzeit nötig, damit der Cluster ordnungsgemäß funktionieren kann. Weitere Informationen über dieses Tool finden Sie auf der <code>ccs_config_dump(8)</code> Handbuchseite. |
| ccs_config_validate — Tool zur Überprüfung der Cluster-Konfiguration | Cluster-Infrastruktur | ccs_config_validate überprüft <code>cluster.conf</code> anhand des Schemas <code>cluster.rng</code> (befindet sich in <code>/usr/share/cluster/cluster.rng</code> auf jedem Knoten). Weitere Informationen über dieses Tool finden Sie auf der <code>ccs_config_validate(8)</code> Handbuchseite. |
| clustat — Dienstprogramm zum Cluster-Status | Komponenten zur Verwaltung von Hochverfügbarkeitsdiensten | Der clustat Befehl zeigt den Status des Clusters an, einschließlich Mitgliedschaftsinformationen, Quorum-Ansicht, und dem Status aller konfigurierten Benutzerdienste. Weitere Informationen über dieses Tool finden Sie auf der <code>clustat(8)</code> Handbuchseite. |
| clusvcadm — Dienstprogramm zur Cluster-Benutzerdienstverwaltung | Komponenten zur Verwaltung von Hochverfügbarkeitsdiensten | Der clusvcadm -Befehl ermöglicht Ihnen das Aktivieren, Deaktivieren, Verlegen und Neustarten von Hochverfügbarkeitsdiensten in einem Cluster. Weitere Informationen über dieses Tool finden Sie auf der <code>clusvcadm(8)</code> Handbuchseite. |
| cman_tool — Tool zur Cluster-Verwaltung | Cluster-Infrastruktur | cman_tool ist ein Programm, das den CMAN Cluster-Manager verwaltet. Es bietet die Funktionalität, um einem Cluster beizutreten, einen Cluster zu verlassen, einen Knoten abzubrechen, oder die erwarteten Quorum-Stimmen in einem Cluster zu ändern. Weitere Informationen über dieses Tool finden Sie auf der <code>cman_tool(8)</code> Handbuchseite. |
| fence_tool — Fencing-Tool | Cluster-Infrastruktur | fence_tool ist ein Programm, das zum Beitreten oder Verlassen einer Fencing-Domain verwendet wird. Weitere Informationen über dieses Tool finden Sie auf der <code>fence_tool(8)</code> Handbuchseite. |

Versionsgeschichte

| | | |
|---|------------------------|----------------------|
| Version 0-4 | 2012-07-18 | Anthony Towns |
| Rebuild for Publican 3.0 | | |
| Version 2.0-1 | Thu May 19 2011 | Steven Levine |
| Release für Red Hat Enterprise Linux 6.1 | | |
| Behebt: #671250 Dokumentiert Unterstützung für SNMP-Traps. | | |
| Behebt: #659753 Dokumentiert den ccs -Befehl. | | |
| Behebt: #665055 Aktualisiert Conga-Dokumentation mit aktualisierter Anzeige und unterstützten Funktionen. | | |
| Behebt: #680294 Dokumentiert die Notwendigkeit des Passwortzugriffs für ricci -Agent. | | |
| Behebt: #687871 Fügt Kapitel zur Suche und Bereinigung von Fehlern hinzu. | | |
| Behebt: #673217 Behebt Tippfehler. | | |
| Behebt: #675805 Fügt Hinweis auf cluster.conf -Schema zu Tabellen der Hochverfügbarkeitsressourcen-Parameter hinzu. | | |
| Behebt: #672697 Aktualisiert Tabellen der Fencing-Geräteparameter, um alle derzeit unterstützten Fencing-Geräte einzubeziehen. | | |
| Behebt: #677994 Korrigiert Informationen für fence_ilo Fencing-Agent-Parameter. | | |
| Behebt: #629471 Fügt technischen Hinweis über das Einstellen des consensus-Werts in einem Zwei-Knoten-Cluster hinzu. | | |
| Behebt: #579585 Aktualisiert Abschnitt über das Aktualisieren der Red Hat Hochverfügbarkeits-Add-On-Software. | | |
| Behebt: #643216 Verdeutlicht einige Sachverhalte im gesamten Dokument. | | |
| Behebt: #643191 Verbessert und korrigiert die luci Dokumentation. | | |
| Behebt: #704539 Aktualisiert die Tabelle der Virtual Machine Ressourcenparameter. | | |
| Version 1.0-1 | Wed Nov 10 2010 | Paul Kennedy |
| Erste Release | | |

Stichwortverzeichnis

A

ACPI

- Konfiguration, [Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten](#)

allgemein

- Überlegungen zur Cluster-Administration, [Allgemeine Überlegungen zur Konfiguration](#)

Arten

- Cluster-Ressource, [Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten](#)

C

Cluster

- Administration, [Vor der Konfiguration des Hochverfügbarkeits-Add-Ons](#), [Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#), [Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit ccs](#), [Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#)
- Fehlerdiagnose und -behebung, [Fehlerdiagnose und -behebung in einem Cluster](#), [Fehlerdiagnose und -behebung in einem Cluster](#)
- Starten, Stoppen und Neustarten, [Starten und Stoppen der Cluster-Software](#)

Cluster-Administration, [Vor der Konfiguration des Hochverfügbarkeits-Add-Ons](#), [Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#), [Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit ccs](#), [Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#)

- Aktivieren von IP-Ports, [Aktivieren von IP-Ports](#)
- Aktualisieren der Cluster-Konfiguration mittels `cman_tool version -r`, [Aktualisieren der Konfiguration mittels `cman_tool version -r`](#)
- Aktualisieren der Cluster-Konfiguration mittels `scp`, [Aktualisieren der Konfiguration mittels `scp`](#)
- Aktualisieren einer Konfiguration, [Aktualisieren einer Konfiguration](#)
- Allgemeine Überlegungen, [Allgemeine Überlegungen zur Konfiguration](#)
- Anzeige von Hochverfügbarkeitsdiensten mit `clustat`, [Anzeige des Hochverfügbarkeitsdienst-Status mit `clustat`](#)
- Cluster-Knoten entfernen, [Ein Mitglied aus einem Cluster löschen](#)
- Cluster-Knoten hinzufügen, [Ein Mitglied zu einem laufenden Cluster hinzufügen](#), [Ein Mitglied zu einem laufenden Cluster hinzufügen](#)
- Cluster-Knoten neu starten, [Einen Cluster-Knoten neu starten](#)
- Einem Cluster beitreten, [Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen](#), [Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen](#)
- Einen Cluster verlassen, [Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen](#), [Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen](#)
- Einen Knoten aus der Konfiguration löschen; Einen Knoten zur Konfiguration hinzufügen, [Hinzufügen oder Löschen eines Knotens](#)
- Fehlerdiagnose und -behebung in einem Cluster, [Fehlerdiagnose und -behebung in einem Cluster](#), [Fehlerdiagnose und -behebung in einem Cluster](#)
- kompatible Hardware, [Kompatible Hardware](#)
- Konfiguration iptables, [Aktivieren von IP-Ports](#)
- Konfiguration von ACPI, [Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten](#)
- Löschen eines Clusters, [Starten, Stoppen, Neustarten und Löschen von Clustern](#)
- NetworkManager, [Überlegungen zum NetworkManager](#)
- Netzwerk-Switches und Multicast-Adressen, [Multicast-Adressen](#)

- Neustarten eines Clusters, [Starten, Stoppen, Neustarten und Löschen von Clustern](#)
- ricci-Überlegungen, [Überlegungen zu ricci](#)
- SELinux, [Red Hat Hochverfügbarkeits-Add-On und SELinux](#)
- Starten eines Clusters, [Starten, Stoppen, Neustarten und Löschen von Clustern](#), [Starten und Stoppen eines Clusters](#)
- Starten, Stoppen und Neustarten eines Clusters, [Starten und Stoppen der Cluster-Software](#)
- Stoppen eines Clusters, [Starten, Stoppen, Neustarten und Löschen von Clustern](#), [Starten und Stoppen eines Clusters](#)
- Überlegungen zur Verwendung von qdisk, [Überlegungen zur Verwendung von Quorum Disk](#)
- Überlegungen zur Verwendung von Quorum Disk, [Überlegungen zur Verwendung von Quorum Disk](#)
- Überprüfung der Konfiguration, [Überprüfung der Konfiguration](#)
- Verwaltung von Cluster-Knoten, [Verwaltung von Cluster-Knoten](#), [Verwaltung von Cluster-Knoten](#)
- Verwaltung von Hochverfügbarkeitsdiensten, [Verwaltung von Hochverfügbarkeitsdiensten](#), [Verwaltung von Hochverfügbarkeitsdiensten](#)
- Verwaltung von Hochverfügbarkeitsdiensten, freeze und unfreeze, [Verwaltung von Hochverfügbarkeitsdiensten mit clusvcadm](#), [Überlegungen zur Verwendung der Freeze- und Unfreeze-Operationen](#)

Cluster-Dienst-Verwaltung

- Konfiguration, [Hinzufügen eines Cluster-Dienstes zum Cluster](#), [Hinzufügen eines Cluster-Dienstes zum Cluster](#), [Hinzufügen eines Cluster-Dienstes zum Cluster](#)

Cluster-Dienste, [Hinzufügen eines Cluster-Dienstes zum Cluster](#), [Hinzufügen eines Cluster-Dienstes zum Cluster](#), [Hinzufügen eines Cluster-Dienstes zum Cluster](#)

- (Siehe auch zur Cluster-Konfiguration hinzufügen)

Cluster-Konfiguration, [Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#), [Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem ccs-Befehl](#), [Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#)

- aktualisieren, [Aktualisieren einer Konfiguration](#)
- Hinzufügen oder Löschen eines Knotens, [Hinzufügen oder Löschen eines Knotens](#)

Cluster-Ressourcenarten, [Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten](#)

Cluster-Ressourcenrelationen, [Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen](#)

Cluster-Software

- Konfiguration, [Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga](#), [Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem ccs-Befehl](#), [Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools](#)

Conga

- Zugriff, [Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software](#)

consensus-Wert, [Der consensus-Wert für totem in einen Zwei-Knoten-Cluster](#)

E

Einführung, [Einführung](#)

- weitere Red Hat Enterprise Linux Dokumente, [Einführung](#)

F

Feedback, [Feedback](#)

H

Hardware

- kompatibel, [Kompatible Hardware](#)

Hochverfügbarkeitsdienst-Konfiguration

- Überblick, [Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten](#)

I

integrierte Fencing-Geräte

- Konfiguration von ACPI, [Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten](#)

IP-Ports

- aktivieren, [Aktivieren von IP-Ports](#)

iptables

- Konfiguration, [Aktivieren von IP-Ports](#)

K

Konfiguration

- Hochverfügbarkeitsdienst, [Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten](#)

M

Multicast-Adressen

- Überlegungen zur Verwendung mit Netzwerk-Switches und Multicast-Adressen, [Multicast-Adressen](#)

N

NetworkManager

- deaktivieren beim Einsatz eines Clusters, [Überlegungen zum NetworkManager](#)

P

Parameter, Fencing-Gerät, [Parameter der Fencing-Geräte](#)

Parameter, Hochverfügbarkeitsressourcen, [Parameter der Hochverfügbarkeitsressourcen](#)

Power-Controller-Verbindung, Konfiguration, [Parameter der Fencing-Geräte](#)

Power-Switch, [Parameter der Fencing-Geräte](#)

- (Siehe auch Power-Controller)

Q

qdisk

- Überlegungen zur Verwendung, [Überlegungen zur Verwendung von Quorum Disk](#)

Quorum Disk

- Überlegungen zur Verwendung, [Überlegungen zur Verwendung von Quorum Disk](#)

R

Relationen

- Cluster-Ressource, [Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen](#)

ricci

- Überlegungen zur Cluster-Administration, [Überlegungen zu ricci](#)

S

SELinux

- Konfiguration, [Red Hat Hochverfügbarkeits-Add-On und SELinux](#)

Suche und Beseitigung von Fehlern

- Fehlerdiagnose und -behebung in einem Cluster, [Fehlerdiagnose und -behebung in einem Cluster](#), [Fehlerdiagnose und -behebung in einem Cluster](#)

T

Tabellen

- Hochverfügbarkeitsressourcen, Parameter, [Parameter der Hochverfügbarkeitsressourcen](#)
- Power-Controller-Verbindung, Konfiguration, [Parameter der Fencing-Geräte](#)

Tools, Befehlszeile, [Überblick über Befehlszeilen-Tools](#)

Totem-Tag

- consensus-Wert, [Der consensus-Wert für totem in einen Zwei-Knoten-Cluster](#)

U

Überprüfung

- Cluster-Konfiguration, [Überprüfung der Konfiguration](#)

V

Verhalten, Hochverfügbarkeitsressourcen, [Verhalten der Hochverfügbarkeitsressourcen](#)