Collax V-Cube+ Fencing Vorgehensweise

Howto

Allgemein

Was ist eigentlich Fencing und für was wird es benötigt?

Falls die Verbindung eines Nodes zu allen anderen Nodes innerhalb des Clusters abbricht, muss eine Komponente im Cluster dafür sorgen, dass der Zugriff auf Cluster-Ressourcen von diesem Node aus unterbunden wird.

Um diese Unterbindung ohne Einschränkungen oder Ausnahmen zu erreichen wird der entsprechende Node ausgeschaltet. Dies dient einzig und allein dem Zweck Daten zu schützen, die durch diese fehlerhafte Node Schaden nehmen könnten. Im Collax Cluster wird dieser Automatismus durch Fencing-Geräte in Form von schaltbaren Steckdosenleisten bewerkstelligt.

Muss ein Fencing-Gerät eingerichtet werden?

Einen Cluster-Verbund ohne funktionierendes Fencing-Gerät zu betreiben kann fatale Folgen haben. Prinzipiell wird ein Produktivbetrieb mit virtuellen Maschinen ohne Fencing-Gerät vom Collax Cluster verhindert, denn das Gerät gilt als Cluster-Ressource und als Basis für den gemeinsamen Festplattenspeicher. Und genau der Letztere muss durch das Fencing-Gerät vor mehrfachem Schreibzugriff geschützt werden, falls sich eine Cluster-Node fehlerhaft verhält. Denn ist das der Fall und mehrere Nodes schreiben in dieselbe Datei, gehen alle Änderungen – bis auf die des letzten Schreibzugriffes – unwiderruflich verloren.

Fencing-Ereignis feststellen

Wenn ein Node durch den Cluster-Manager aus einem bestimmten Grund ausgeschaltet wird, so ist das durch die Hochverfügbarkeit im Cluster-Verbund zunächst kaum zu bemerken. Denn alle laufenden virtuellen Maschinen wurden sofort nach dieser Aktion im Cluster auf anderen Nodes gestartet.

In diesem Fall werden E-Mails an die hinterlegte E-Mail-Adresse des Administrators gesendet, in denen der Status der Dienste von des ausgeschalteten Cluster-Nodes als *CRITICAL* bezeichnet sind. Zusätzlich ist der Status des betreffenden Cluster-Nodes auf Non-member (offline) gesetzt. Der letzte Beweis für ein stattgefundenes Fencing-Ereignis sieht man in der Administration des Fencing-Devices selbst. Dort sind die entsprechenden Steckdosen ausgeschaltet.

Fencing Funktionalität überprüfen

Vor Inbetriebnahme Ihres Cluster sollte gewährleistet sein, dass die von Ihnen eingerichteten

Steckdosenleisten korrekt funktionieren und keine Fehlkonfiguration vorliegt. Bei einer vertauschten Verkabelung oder Dosenkonfiguration würden sich zum Beispiel beide Nodes gegenseitig ausschalten. Um die Funktionalität ihrer Fencing-Lösung zu überprüfen folgen Sie bitte diesen Schritten.

- Setzen Sie Ihren zweite Cluster-Node auf Standby, beenden Sie den HA-Cluster Dienst und fahren Sie den Node anschließend herunter.

Hinweis: Bei diesem Test wird keiner Ihrer Cluster-Nodes wirklich „abgeschossen". Es wird lediglich eine Dose abgeschaltet an der eine bereits gezielt ausgeschaltete Node angeschlossen ist.

- Setzen Sie daraufhin auch Ihren ersten Node auf Standby und beenden Sie auch dessen HA-Cluster Dienst.
  Dass diese Aktionen erfolgreich waren erkennen sie daran, dass die Formulare Cluster Nodes, Cluster Ressourcen und Cluster Monitor dementsprechende Warnhinweise bringen.
- Nun starten Sie auf der ersten Node den HA-Cluster Dienst wieder und setzen den Node daraufhin von Standby zurück auf Aktiv. Der Node weiß nun nicht mehr, dass ihre zweite Cluster-Node korrekterweise ausgeschaltet ist, und schaltet ihn mittels Fencing aus.
- Über die Webadministration Ihrer Steckdosenleiste sollten sie nun erkennen können, dass der Dose in der Ihre zweite Node steckt der Strom abgedreht wurde. Der Test war erfolgreich.

- Nach diesem Test können Sie die gerade abgeschaltete Dose über die Weboberfläche der Steckdosenleiste unter Strom setzen und den zweiten Node wieder hochfahren.
- Starten Sie dort den HA-Cluster Dienst und warten Sie bis die Verbindung zum Cluster erfolgreich aufgebaut wurde, der Node also wieder als online ausgewiesen wird.
- Nun können Sie den zweite Node wieder aus dem Standby-Modus nehmen und aktiv setzen. Kontrollieren Sie anschließend ob ihre DRBDs erfolgreich und vollständig synchronisiert wurden.

Nach einer Fencing-Aktion

Wenn ein Node ausgeschaltet wurde, liegt ein Defekt vor. In der Vorgehensweise liegt also die Ursachenanalyse dieses Defekts ganz vorn. Denn wird der Fehler nicht behoben, schaltet das Fencing-Gerät den Node wieder aus, um die Datenintegrität zu gewährleisten.

Neuinstallation

Ein besonderer Fall an dieser Stelle tritt ein, wenn der Node neu installiert werden muss. Hier konsultieren Sie bitte im Dokument zum Hardware-Tausch im Cluster-Verbund das Kapitel „Wartung mit Neuinstallation".

Node hochfahren

Um den Node überhaupt starten zu können muss er über das Fencing-Gerät wieder mit Strom versorgt werden. Diese Einstellung können Sie auf der Administrationsoberfläche vornehmen. Wenn der Node noch starten kann, ist hier im Bootmenü die Option *Filesystem Check* auszuführen. Wenn dies soweit erfolgreich durchgeführt wurde, startet der Node. Dieser Node startet mit dem Cluster Status *Offline*, er wird also nicht als Ressourcen-Träger im Cluster genutzt.

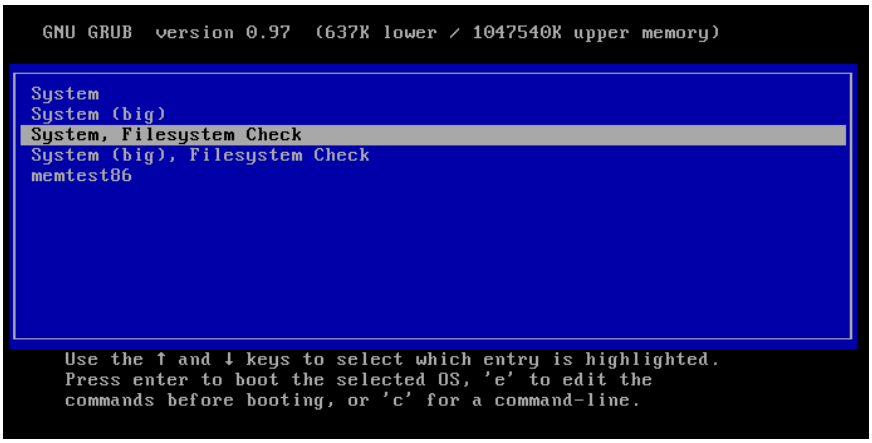

Abbildung 1: Filesystem Check im Bootmenü auswählen.

Ursache suchen und beheben

Bei der Suche nach der Ursache hilft die Prüfung des Interconnects und der LAN-Anbindung, um festzustellen, ob ein Netzwerkgerät defekt ist. Prüfen sie zusätzlich in System-Logfiles und / oder kontaktieren Sie Collax, um die Ursache herauszufinden. Folgende Bereiche sind zu diesem Zeitpunkt in Augenschein zu nehmen, da sie zum Ausschalten eines Nodes führen:

- Mainboard (z.b. Firmware), RAID-Controller, Festplatten, RAM
- Netzwerk/Ethernet/Verkabelung auf Interconnect-Verbindung
- Spannungsversorgung

Cluster Share – OCFS2-Dateisystem prüfen

Eine Prüfung des Dateisystems des Cluster Shares ist dann erforderlich, wenn kurz vor dem Fencing-Ereignis

- Virtuelle Maschinen mit Diskimage-Dateien
- Virtuelle Maschinen mit Snapshots

im Cluster betrieben wurden. Diskimage-Dateien oder Snapshots werden innerhalb des OCFS-Dateisystem abgelegt.
Eine Prüfung des OCFS-Dateisystems benötigt immer eine geplante Ausfallzeit der virtuellen Maschinen.
Gehen Sie für den OCFS2-Dateisystemcheck wie folgt vor, wenn Sie die Fehlerursache im Kapitel 2.3 behoben haben:

- Fahren Sie alle virtuellen Maschinen im Cluster herunter.

  Falls ein Node noch ausgeschaltet ist:
  - Starten Sie den noch ausgeschaltenen Cluster Node
  - Starten Sie den Dienst HA-Cluster des betreffenden Nodes
  - Setzen Sie den Node im Dialog *Cluster Nodes* aktiv.

- Stoppen Sie die Ressource OCFS im Dialog *Cluster Ressourcen*
- *Führen Sie nun folgenden Befehl in der root-Befehlszeile auf einem der Nodes aus:*

  ```
  fsck.ocfs2 -yf /dev/drbd/by-res/CLUSTER-SHARE-NAME
  ```
  Der Zeitbedarf für die Prüfung liegt zwischen wenigen Sekunden (<500GB) bis wenigen Minuten (<4TB) Die Dateisystemprüfung darf in diese Zeit auf keinen Fall unterbrochen werden.

- Wenn die Prüfung beendet wurde, starten Sie im Dialog *Cluster Ressourcen* die Ressource OCFS

wieder.

- Die virtuellen Maschinen können nun wieder gestartet werden

Abschließende Schritte

Diese Schritte sind nur durchzuführen, wenn die Ursache für das Auslösen der Fencing-Aktion behoben wurde. Nun kann der betreffende

- Node im Dialog *Cluster Nodes* in den Modus *Standby* gesetzt
- und der Dienst HA-Cluster im Dialog *Cluster-Dienste* gestartet werden. Achten sie darauf, dass alle Dienste wieder gestartet werden.

Zurück im Dialog *Cluster Nodes* kann die Node aktiv wieder in den Cluster-Verbund aufgenommen werden.

Falls Embedded SAN Festplatten für virtuelle Maschinen benutzt werden, beginnt der Cluster diese Festplatten auf den eben aktivierten Node zu synchronisieren. Anschließend werden VMs mit Präferenz auf diesen Node automatisch migriert.

Für Fragen zu der Vorgehensweise wenden Sie sich an das kompetente Collax Support Team.