# 集群脑裂

## 简介

在“双机热备”高可用（HA）系统中，当联系2个节点的“心跳线”断开时，本来为一个整体、动作协调的HA系统，就分裂为2个独立的个体。由于相互失去了联系，都以为是对方出现了故障，2个节点上的HA软件像“裂脑人”一样，本能地争抢共享资源、争起应用服务，这样就会发生严重后果：或者共享资源被瓜分、两边服务都起不来了；或者两边服务都起来了，但同时读写共享内存，导致数据损坏（常见的如数据库轮询着的联机日志出错）。

## HeartBeat

运行于备用主机上的HeartBeat可以通过以太网连接检测主服务器的运行状态，一旦其取法检测到主服务器的“心跳”则自动接管主服务器的资源。通常情况下，注、备服务器间的心跳连接是一个独立的物理连接，这个连接可以是串行线缆、一个由“交叉线”实现的以太网连接。HeartBeat甚至可同时通过多个物理连接检测主服务器的工作状态，而其只要能通过其中一个连接收到主服务器处于活动状态的信息，就会认为主服务器处于正常状态。

从实践经验的角度来看，建议为HeartBeat配置多条独立的物理连接，以避免HeartBeat通信线路本身存在单点故障。

## 连接方式

1. 串行电缆：被认为是比以太网连接安全性稍好些的连接方式，因为hacker无法通过串行连接运行诸如telnet、ssh或者rsh类的程序，从而可以降低其通过已劫持的服务器再次侵入备份服务器的几率。但串行线缆受限于可用长度，因此主、备服务器的举例必须非常短；
2. 以太网连接：使用此方式可以消除串行线缆在长度方面的限制，因此可以通过此连接主、备服务器间同步文件系统，从而减少了从正常通信连接带宽的占用

基于冗余的角度考虑，应该在主、备服务器使用两个物理连接传输HeartBeat的控制信息，这样可以避免在一个网络或者线缆故障时导致两个节点同时认为自己是唯一处于活动状态的服务器，从而出现争用资源的情况，这样争用资源的场景就是所谓的“脑裂”（split-brain）或“partitioned luster”。在两个节点共享同一个物理设备资源的情况下，脑裂会产生相当可怕的后果。

## 预防措施

为了避免出现脑裂，可采用如下的预防措施：

1. 添加冗余的心跳线，例如双心跳线，尽量减少“脑裂”发生几率；
2. 启动磁盘锁，正在服务一方锁住共享磁盘，“脑裂”发生时，让对方完全“抢不走”共享磁盘资源。但使用磁盘锁也会有一个问题，如果占用共享盘一方不主动“解锁”，另一方就永远得不到共享盘。现实中假如服务节点突然死机或崩溃，就不可能执行解锁命令。后备节点也就接管不了共享资源和应用服务。于是有人在HA中设计了“智能锁”，即正在服务的一方只要发现心跳线全部断开（觉察不到对端）时才启用磁盘锁，平时就不上锁。
3. 设置仲裁机制，例如设置参考IP（例如网关IP），当心跳完全断开时，2个节点都各自ping一下参考IP，不通则表明断点就出在本端，不仅“心跳”、还兼对外“服务”的本端网络链路断了，即使启动（或继续）应用服务也没有用了，那就主动放弃竞争，让能够ping通参考IP的一端去启动服务。更保险一些，ping不通参考IP的一方干脆自动重启，以彻底释放可能还占用着的那些共享资源。

# fence

## 简介

fence是RHCS的HA集群中预防集群出现脑裂之后节点争抢文件系统的一种手段。

红帽的HA集群中没有可用的fence设备（例如HP ilo，IBM ipmi以及DELL drac5/6），那么当集群心跳线断开或者物理机宕机，则服务无法自动切换。使用手动fence的，当节点关机的时候服务是可切换的，但是当节点宕机或者断网，切换就不行了。必须要用fence\_ack\_manual去人工干预，而且这相当于用欺骗另外一个节点已经被fence掉，而不管对方是不是真正被fence。所以从这个角度讲，没有fence，无法构建一个完整的RHCS HA集群。而且如果使用没有fence设备的服务器或者环境去搭建RHCS HA集群的时候，红帽官方不会提供技术支持。因此，fence设备是必须的。

## 设备

现在常用的fence设备，除了上述的不同品牌自带的之外，还有一些电源管理交换机，如WTI或者APC。针对虚拟化场景，如果你的host使用的是RHEL，那么可以使用fence\_xen或者fence\_virsh（分别针对Xen和KVM架构），针对host是VMware ESX的，可以使用fence\_vmware\_soap，不过操作系统必须是RHEL6.1以上，另外某些环境可以使用存储fence，即通过阻塞光纤交换机的接口来起到禁止被fence的机器访问存储的效果，不过不能够做到自动化，阻塞的端口必须得手动打开。

如果集群中一个节点通信失效，那么集群中的其他节点必须能够保证将已经失效的节点与其正在访问的共享资源隔离开，出问题的集群节点本身无法做到这一点，因为该集群节点在此时可能已经失去响应（例如发生hung机），因此需要通过外部机制实现这一点，这种方法被称为带有fence代理的隔离。

不配置隔离设备，我们没有办法知道之前断开连接的集群节点使用的资源是否已经被释放掉。如果我们没有配置隔离代理（或设备），系统可能错误地认为集群节点已经释放了它的资源，这将会造成数据损坏和丢失。没有配置隔离设备，数据的完整性就不能够被保证，集群卑职将不被支持。

当隔离动作正在进行中时，不允许执行其他集群操作。这包括故障转移服务和获取GFS文件系统或GFS2文件系统的新锁。在隔离动作完成之前或在该集群节点已经重启并且重新加入集群之前，集群不能恢复正常运行。

隔离代理（或设备）是一个外部设备，这个设备可以被集群用于限制异常节点对共享存储的访问（或者硬重启此集群节点），两类最常用的隔离设备是：

1. 电源隔离设备：集群软件通过telnet、ssh或SNMP登录到比如APC交换机，DELL DARC，IBM RSA，禁用（或者开启）集群节点的电源，这个方法将会执行一个“硬关闭”操作，一些隔离代理将需要设置acpi be disabled。
2. I/O隔离代理：集群软件通过telnet或者ssh登录到光纤通道交换机，关闭相应节点的端口，以切换其对共享存储的访问，这种方式需要管理员手动重启或关闭异常的节点来恢复它，并且登录到交换机界面重启对应的端口，这也可以通过SCSI保留隔离实现。

## 配置

配置集群的一些要求：

1. 隔离设备是所有集群节点都需要的；
2. 隔离代理fence\_manual是一个不支持的隔离设备，仅用于测试；
3. 将要被隔离的集群节点必须能够访问所有的隔离设备，不考虑集群节点的电源状态。例如，如果将要被隔离的集群节点正在使用板载系统管理口（比如ilo/drac/rsa），那么隔离设备必须有一个外部的电源以便当计算机没有电力供应，隔离设备仍然有电力供应。

隔离是RedHat集群基础设施的基础部分，因此验证或测试隔离动作能有效完成，有足够的冗余比如配置多个隔离设备及拥有适度的弹性（可靠性和可用隔离机制）是很重要的，RedHat建议使用备用的隔离设备。