

Sistemas informaticos redundantes

Autor:
WWW Ibercom, S.L.

Creado en: 25 Sep 2006 08:56 AM

En este artículo vamos a ver una introducción de diferentes técnicas que se utilizan para que los sistemas informáticos estén disponibles y se puedan acceder incluso cuando alguna parte del sistema falla.

Cuando se tienen sistemas críticos que tienen que estar disponibles y funcionando 24 horas al día, 365 días al año, hay que intentar minimizar los fallos que puedan afectar al funcionamiento normal del sistema. Fallos van a ocurrir, pero existen técnicas y configuraciones que ayudan a tener sistemas redundantes, en los que ciertas partes pueden fallar sin que esto afecte al funcionamiento del mismo.

En un sistema informático actual, existen muchos componentes necesarios para que este funcione, cuantos más componentes, más probabilidad tenemos que algo falle. Estos problemas pueden ocurrir en el propio servidor, fallos de discos, fuentes de alimentación, tarjetas de red, etc. y en la infraestructura necesaria para que el servidor se pueda utilizar, componentes de red, acceso a Internet, sistema eléctrico,....

A continuación vamos a ir comentando algunas de las técnicas usadas para obtener sistemas redundantes. El grado de redundancia de un sistema, dependerá de su importancia y del dinero que perdamos cuando el sistema no está disponible por un fallo. No nos merecerá la pena invertir en 'redundancia', si la inversión necesaria para tener un sistema redundante cuesta más de lo que perderíamos en dinero, reputación y horas de trabajo, si el sistema fallara.

Las técnicas y configuraciones de las que hablamos a continuación no son exclusivas de sistemas Linux. Se pueden aplicar en su gran mayoría a otros sistemas operativos y plataformas.

Redundancia de componentes en el servidor

Los componentes redundantes más normales en un servidor suelen ser, los discos, las tarjetas de red y las fuentes de alimentación. Existen servidores con múltiples PCUS que incluso siguen trabajando sin problemas con alguna CPU o módulo de memoria estropeado.

Discos

Los discos duros son los dispositivos donde se graban los datos. El fallo más común en un servidor es el fallo de un disco duro. Si el servidor tiene solamente un disco y este falla, fallará el servidor al completo y no podremos acceder a los datos contenidos en el mismo. Existen por ello técnicas que nos ayudan a minimizar este problema y a que el servidor siga funcionando y no pierda datos incluso cuando falle algún disco duro. Lo más normal también, es que se puedan sustituir los discos que fallan sin necesidad de apagar el servidor.

La técnica más común es la llamada RAID (redundant array of independent disks). Con esta técnica creamos un conjunto de discos redundantes que nos pueden ayudar, tanto a aumentar la velocidad y el rendimiento del sistema de almacenamiento, como a que el sistema siga funcionando aunque algún disco falle. Existen implementaciones por software y hardware y diferentes configuraciones RAID, siendo las más comunes RAID1, RAID5 y RAID10.

Tarjetas de red

La tarjeta de red es el dispositivo que permite al servidor comunicarse con el resto del mundo. Es por ello muy común que los servidores tengan como mínimo dos tarjetas de red, para garantizar que esta comunicación no se corte en caso de fallo de una de las tarjetas.

En Linux existe además una técnica llamada "Bonding", por la cual podemos utilizar dos o más tarjetas de red como si fueran un único dispositivo, sumando las capacidades de las mismas y teniendo redundancia en el caso que alguna de las tarjetas falle.

Fuentes de alimentación

La fuente de alimentación es la encargada de proporcionar electricidad al servidor. También es común que los servidores tengan dos o más fuentes de alimentación conectadas a diferentes sistemas eléctricos, para garantizar el suministro en el caso que una de las fuentes o uno de los sistemas eléctricos fallen. Lo más normal es que se puedan sustituir las fuentes de alimentación que fallan sin necesidad de apagar el servidor. Otros componentes del sistema como rotures, switches, gabinetes de discos, etc. suelen utilizar la misma técnica de redundancia.

Redundancia en el suministro eléctrico

Todo componente eléctrico, y un servidor no podía ser menos, necesita un suministro constante de electricidad para funcionar. Fallos en este suministro, aunque sean por periodos muy cortos de tiempo, tendrá consecuencias catastróficas para nuestro sistema. Y no solo necesitamos un suministro constante, también necesitamos que no tenga subidas y bajadas brusquedad que puedan estropear componentes electrónicos.

Para conseguir esto se pueden utilizar diferentes componentes según el grado de protección que deseemos.

SAI (UPS): Son baterías más o menos avanzadas que se conectan entre el servidor y la fuente de suministro eléctrico. Garantizan un suministro constante y estable por un tiempo, dependiendo este de la capacidad de las mismas.

Generadores eléctricos: Funcionan generalmente con diesel y se conectan entre los UPS y la red de suministro eléctrico. Solo entran en funcionamiento cuando el suministro se corta por más de un determinado tiempo. Pueden suministrar electricidad por un tiempo indefinido siempre que tengan carburante en el tanque.

Líneas independientes de suministros: En centros de datos grandes, se suelen tener al menos dos conexiones diferentes e independientes a la red de suministro eléctrico.

Si queremos redundancia en el sistema eléctrico, no hace falta decir que no solo los servidores tienen que tener dobles conexiones, rotures, switches y en definitiva cualquier componente del sistema que utilice electricidad debería de tener fuentes de alimentación redundantes (conectadas). Como se suele decir, tu sistema solo será tan seguro, estable y redundante como el componente más débil del mismo. No es la primera vez, por ejemplo, que en un centro de datos, grupos de servidores con redundancia a todos los niveles han quedado incomunicados porque estaban conectados a un switch que ha fallado por no tener un sistema redundante de suministro eléctrico.

Redundancia en los componentes de red

De nada sirve tener servidores con componentes duplicados y redundantes y un suministro eléctrico constante y equilibrado si algunos de los componentes de la red fallan y no podemos acceder al servidor.

Los componentes más normales en una red son:

Router (**enrutador**): Es un dispositivo que interconecta segmentos de red o redes enteras

Switch (**Conmutador**): Es un dispositivo que interconecta dos o más segmentos de red

Tarjeta de red ó **NIC**: Es un dispositivo electrónico que permite a una DTE (Data Terminal Equipment), ordenador o impresora, acceder a una red y compartir recursos

Cables de red: Para interconectar los diferentes componentes, existen muchos y variados tipos, siendo los más comunes el cable de par trenzado y el de fibra óptica

Líneas de conexión: a la red de área amplia, WAN (por ejemplo Internet)

Cualquiera de estos componentes puede fallar, dejando al sistema incomunicado. Pero existen técnicas para evitar que esto ocurra, lo que se suele hacer es configurar la red, para que al menos existan 2 caminos diferentes entre dos componentes A y B. En el gráfico siguiente tenéis un esquema, en el que podéis ver como configurar una red con redundancia doble desde el servidor hasta Internet. De esta manera se puede estropear un router, un switch y una tarjeta de red a la vez sin que perdamos conectividad. El mismo esquema se podría ampliar para tener redundancia triple o cuádrupla de los componentes.

Redundancia de servidores, balanceo de cargas

Que ocurre si el suministro eléctrico funciona y la red funciona, pero nuestro servidor falla de tal manera que ninguno de los componentes redundantes que tiene pueda evitar el fallo y la caída del mismo. Existen diferentes tipos de configuraciones con varios servidores, que pueden ayudarnos con este problema. Son los llamados clusters, los hay de diferentes tipos, pero entre los más útiles está el de balanceo de cargas con tolerancia a fallos. En este tipo de clusters, no solo no importa que uno o varios de los servidores deje de funcionar, sino que si necesitamos más recursos para proporcionar un servicio, podemos incorporar nuevos servidores que incrementen la capacidad de proceso del cluster.

Los componentes más importantes de este tipo de clusters son, los sistemas de almacenamiento únicos entre todos los servidores que proporcionan un servicio y el dispositivo de balanceo de cargas, el cual puede ser un hardware específico para este trabajo o implementarse por software en un servidor normal. El proyecto para Linux más importante sobre este tema es el denominado Linux Virtual Server (LVS).

A continuación tenéis una serie de ejemplos de como se pueden organizar estos clusters, en donde el fallo de un servidor, no para el funcionamiento de un servicio. Cuando falla uno o varios servidores en el cluster, la capacidad de proceso del mismo se reduce, por lo que es importante tener siempre cierta capacidad sin usar para que en el caso de un fallo no se reduzca el tiempo de respuesta mucho.

En fin, esto es todo lo que tenía pensado contar en esta introducción a sistemas informáticos redundantes. Existe mucha información en Internet si queréis profundizar en el tema. Lo más importante es tener conocimientos, de red y administración y saber como funcionan los diferentes componentes de un sistema. La experiencia y estudios de estas materias os ayudaran a tener sistemas más estables y redundantes.

Fuente: <http://www.linux-es.org>