Brenda Fuentes Vázquez 4CV2

Sistemas distribuidos de tolerancia a fallas / alta disponibilidad (DFT / HA)

Las plataformas de telecomunicaciones deben proporcionar disponibilidad de "cinco nueves"(99.999 por ciento), lo que significa prácticamente ninguna pérdida de servicio debido a errores de hardware o software, ni ningún tiempo de inactividad para las actualizaciones de software o el mantenimiento de hardware. El soporte depende de la interacción casi impecable del software, el hardware y el diseño de la red, así como también de los factores ambientales y operativos.

Conceptos de FT / HA (Fault-Tolerant / High-Availability)

Alta disponibilidad

Para comprender la disponibilidad, primero debemos comprender la fiabilidad. Un sistema puede considerarse altamente confiable (puede fallar con poca frecuencia), pero no se considerará altamente disponible. Una medida de la confiabilidad de un elemento es su índice de falla, o Tiempo Medio hasta la Falla (MTTF), el intervalo en el que el sistema o elemento puede proporcionar el servicio sin falla. Otra medida de confiabilidad es el Tiempo Medio de Reparación (MTTR), que representa el tiempo que toma reanudar el servicio después de que se ha experimentado una falla.

La disponibilidad de los sistemas se puede aumentar mediante el diseño de componentes que sean altamente confiables (alto MTTF), y / o acortando el tiempo requerido para reparar el sistema y devolverlo al servicio (MTTR bajo).

Disponibilidad = MTTF / (MTTF + MTTR)

Tolerancia a fallos

Un sistema tolerante a fallas está disponible en presencia de fallas. La estrategia más simple de respuesta a fallas es dejar que un sistema no redundante falle y luego repararlo fuera de línea. Esta es la estrategia de menor disponibilidad.

Una forma de lograr la tolerancia a fallas del sistema es usar componentes de hardware redundantes dentro del sistema que operan simultáneamente y en paralelo, comparando los resultados de las operaciones realizadas. Cuando un subsistema falla debido a la presencia de una falla, el otro subsistema toma el control, de modo que el sistema en general puede seguir funcionando sin interrupción en el servicio.

Soluciones de hardware FT / HA

El tipo más simple de elemento de red no es redundante y debe repararse fuera de línea si falla. Este tipo de elemento tendrá una complejidad de diseño relativamente baja y un bajo costo. La tolerancia a fallas del hardware generalmente depende de procesadores redundantes, memoria, buses, conexiones cruzadas de bus, fuentes de alimentación, sistemas de enfriamiento y almacenamiento en disco.

Los elementos con redundancia adicional suelen utilizar "reintentar" y "enmascarar" para la recuperación. Los elementos basados en reintentos intentan asegurar que hay un segundo intento en la

operación si falla una operación inicial. Si el segundo intento tiene éxito, la falla probablemente fue transitoria. Si el segundo intento falla, la falla probablemente sea permanente. Los elementos basados en enmascaramiento intentan garantizar que solo se utilicen los resultados de la parte operativa correcta del elemento si falla un componente. En cualquier caso, si un componente ha fallado, el sistema intenta detectar, diagnosticar, aislar, recuperar, reparar y compensar la falla.

El software de gestión de fallas gestiona la conmutación del nodo fallido a otro nodo operacional, manteniendo la información de estado del nodo fallido para que pueda ser utilizado por el sistema después de la conmutación.

En la arquitectura de nodo dual, dos nodos se ejecutan simultáneamente. En algunos sistemas, ambos nodos están activos. En otros sistemas, un nodo se asigna para estar activo y el otro nodo está en modo de espera. Una arquitectura multinodo más escalable permite que se configuren la cantidad de nodos activos y en espera y que los nodos activos compartan la carga del sistema.

Un sistema de doble nodo generalmente logra tolerancia a fallas en una de dos formas:

• Ambos nodos están activos, compartiendo la carga del sistema mediante la ejecución de diferentes tareas. Si un nodo activo falla, el otro nodo activo asume las tareas del nodo fallido.

• Ambos nodos son capaces de ejecutar las mismas tareas, pero un nodo está activo y el otro está en modo de espera. Si el nodo activo falla, el nodo en espera se activa y asume las tareas asignadas.

Tres esquemas de redundancia comunes encontrados en soluciones basadas en hardware son:2N: un nodo en espera para cada nodo en operación, N + 1: un nodo en espera para N nodos operativos. , N + M: un conjunto de N nodos que trabajan en funcionamiento normal con un grupo de M nodos en el modo de espera.