Alta disponibilitat

UF4

Mesures, MTBF i redundància

ALTA DISPONIBILITAT

M11 Seguretat i alta disponibilitat

CURS 2015 - 2016

Hèctor López
hector.lopez@fje.edu

JESUÏTES El Clot
Escola del Clot

Alta disponibilitat

Seguretat informàtica

Quan parlem de seguretat informàtica, estem parlant en definitiva de:

- **Fiabilitat**: funcionament correcte dels sistemes, realitzant les tasques tal com han estat previstes.
- **Confidencialitat**: garantir que l'accés a les dades del sistema està restringit únicament a les persones autoritzades.
- **Integritat**: assegurar que les dades del sistema no han estat manipulades per persones no autoritzades i que per tant no s'han vist alterades.
- **Disponibilitat**: capacitat del sistema per ser accessible i operatiu el màxim de temps possible.

Alta disponibilitat

Sistemes d'alta disponibilitat

Els sistemes d'**alta disponibilitat** són doncs, sistemes informàtics que han estat dissenyats seguint un conjunt de normes i tècniques per tal que el sistema pugui estar disponible sempre o, si més no, **el màxim de temps possible**.

Aconseguir que els sistemes informàtics estiguin disponibles sempre és gairebé **utòpic**, ja que són molts els riscos que s'han de tenir en compte. No obstant això, les empreses preparen els seus sistemes per tal que estiguin disponibles el màxim temps possible.

Les empreses són cada cop més dependents dels seus sistemes informàtics i, per tant, una **aturada en els servidors** els pot suposar **elevades pèrdues** tant **econòmiques** com **materials**.

És per aquest motiu que cal dissenyar adequadament els sistemes informàtics de manera que es trobin disponibles en els moments en què són necessaris.

Alta disponibilitat

Sistemes d'alta disponibilitat

Per tal que els sistemes informàtics tinguin una elevada disponibilitat caldrà implantar solucions de **programari** i de **maquinari**. Cal tenir present que la majoria de solucions d'alta disponibilitat comporten uns **costos força elevats**.

vs.

Sistemes d'alta disponibilitat

Aturades planificades

Determinades tasques de manteniment que realitzen els administradors (com actualitzacions, canvis de configuració o algunes còpies de seguretat) provoquen que els sistemes deixin d'estar operatius durant uns minuts. Aquest tipus d'aturades és el que s'anomenen **aturades planificades**, ja que els administradors les planifiquen per realitzar en moments que puguin tenir poc impacte en el funcionament de l'empresa. Estan controlades i es coneix per endavant la durada que tindran.

Aquest tipus d'accions que generen un **temps d'inactivitat** s'acostumen a fer per les nits o en cap de setmana per tal d'afectar el mínim nombre d'usuaris, i sempre es notifiquen per endavant.

Sistemes d'alta disponibilitat

Aturades no planificades (I)

Aquests poden ser causats per diversos factors. A continuació n'identifiquem alguns dels possibles riscos que caldrà tenir en compte:

- **Fallades de maquinari**: el sistema deixarà d'estar operatiu si es produeix una aturada en algun dels dispositius bàsics del servidor com són la font d'alimentació, el disc dur o bé la memòria.
- **Talls i fluctuacions del subministrament elèctric**: poden ser produïts per una fallada en les fonts d'alimentació locals, fluctuacions de tensió (pujades o caigudes de tensió), o talls totals en el subministrament elèctric.
- **Pèrdua o bloqueig de la informació**: la informació del sistema pot ser inaccessible ja sigui per un atac o bé per una mala gestió dels usuaris.

Sistemes d'alta disponibilitat

Aturades no planificades (II)

Aquests poden ser causats per diversos factors. A continuació n'identifiquem alguns dels possibles riscos que caldrà tenir en compte:

- **Fallades en la infraestructura de comunicacions**: avui en dia la majoria de sistemes informàtics estan formats per la unió de diferents dispositius en una xarxa comuna. Un tall en la infraestructura de comunicacions suposarà la fallada del sistema complet, tant si es tracta de comunicacions locals com de comunicacions entre centres.

- **Saturació en els servidors de processament de dades**: sovint, el bloqueig del servidor per un volum de dades superior al que és capaç de gestionar pot suposar una caiguda del sistema.

Sistemes d'alta disponibilitat

Temps d'inactivitat

Així doncs, el **temps d'inactivitat** és el període de temps en què el nostre sistema no està operatiu i, per tant, no pot respondre a les peticions que realitzin els usuaris. En funció de les causes podem diferenciar dos tipus de temps d'inactivitat: **planificat** o **no planificat**.

$$t_{inactivitat} = t_{planificat} + t_{no\_planificat}$$

Sistemes d'alta disponibilitat

Mesura

Per tal de mesurar l'alta disponibilitat s'ha creat una **mètrica de càlcul**, vàlida per a tots els sistemes informàtics.

Primer de tot, cal establir quina hauria de ser la disponibilitat del nostre sistema. Això és el que s'anomena **acord del nivell de servei** (**SLA**, en anglès, *Service Level Agreement)*.

L'acord del nivell de servei pot variar de *8x5* a *10x5*, en funció dels horaris dels treballadors, o fins a un *24x365*, en sistemes que necessiten estar operatius tots els dies de l'any les 24h del dia. Aquests també poden anomenar-se *24/7*.

Sistemes d'alta disponibilitat

Mesura

Els **SLA**, o acords del nivell de servei s'acostumen a utilitzar per establir un **contracte** entre un proveïdor de servei i un client. En aquest contracte s'estableixen els nivells mínims de qualitat en base a diferents aspectes:

- Temps de resposta.
- Disponibilitat horària.
- Personal assignat.
- etc.

Bàsicament, es realitzen contractes d'aquest tipus amb empreses de telecomunicacions i serveis externalitzats.

Alta disponibilitat

Sistemes d'alta disponibilitat

Mesura

%disponibilitat = ((X – Y) / X) * 100

On:

→ **X** representa el nombre d'**hores que el sistema hauria d'estar operatiu** en referència a l'acord de nivell de servei de l'empresa i

→ **Y** representa les **hores d'inactivitat del sistema**.

Sistemes d'alta disponibilitat

Càlcul de l'índex de disponibilitat – *Exercici* –

El cap d'informàtica d'un hospital ens ha demanat que calculem l'**índex de disponibilitat** del servidor on es troben emmagatzemats els expedients mèdics de tots els pacients.

L'hospital disposa de servei d'urgències, que està obert les **vint-i-quatre hores del dia tots els dies de l'any**. Perquè els metges del servei puguin consultar els expedients mèdics s'han implantat algunes mesures d'alta disponibilitat, no obstant això, al llarg de l'any el servidor ha tingut un **temps d'inactivitat** acumulat de 53 minuts i 14 segons. El cap ens comenta que un índex de disponibilitat inferior a un 99,99% seria insuficient per al servidor de l'hospital.

Sistemes d'alta disponibilitat

Càlcul del temps d'inactivitat – *Exercici* –

En una gestoria on els treballadors fan un horari laboral de **nou del matí a sis de la tarda**, el servidor on s'emmagatzemen les dades de comptabilitat té un **índex de disponibilitat del 99%**.

Quin **temps d'inactivitat** màxim ha acumulat el servidor al llarg de l'any per arribar a aquest índex d'inactivitat?

Alta disponibilitat

Sistemes d'alta disponibilitat

Relació entre l'índex de disponibilitat i el temps d'inactivitat – *Exercici* –

En una empresa d'allotjament web disposen actualment d'un **índex de disponibilitat del 99%**. Han rebut una oferta força interessant econòmicament d'una agència de viatges que opera per Internet. No obstant això, per acabar utilitzant els seus serveis exigeixen un **índex de disponibilitat no inferior al 99'99%**.

Com s'hauria de **reduir el temps d'inactivitat** per tal que l'agència de viatges accepti allotjar el seu web en el servidor d'aquesta empresa?

Alta disponibilitat

Sistemes d'alta disponibilitat

Disponibilitat	Temps inactiu/any	Temps inactiu/mes	Temps inactiu/dia
90%	36,5 d	73 h	2,4 h
95%	18,3 d	36,5 h	1,2 h
98%	7,3 d	14,6 h	28,8 min
99%	3,65 d	7,3 h	14,6 min
99,9%	8,8 h	43,8 min	1,46 min
99,99%	52,6 min	4,4 min	8,8 s
99,999%	5,3 min	26,3 s	0,9 s
99,9999%	31,5 s	2,6 s	0,08 s

Taula: Relació entre % de disponibilitat i temps d'inactivitat per any, mes i dia d'un sistema 24×365

Alta disponibilitat

Solucions d'alta disponibilitat

Un cop s'han identificat els possibles riscos als quals pot estar sotmès un sistema informàtic s'han d'implantar les solucions adients per evitar o mitigar el seu impacte. Les empreses que necessitin garantir una major disponibilitat dels seus serveis hauran d'incrementar les inversions en aquest àmbit per tal de cobrir totes les possibles circumstàncies.

Podem trobar solucions de tot tipus: des de **redundància en els dispositius** de maquinari a **redundància en les comunicacions**, passant per **centres de processament de dades secundaris** i **plans de contingència**.

Anem a analitzar-los detingudament un per un...

Solucions d'alta disponibilitat

Redundància en el maquinari (I)

Un dels riscos que en cas de manifestar-se pot comportar uns majors temps d'inactivitat són les **fallades en el maquinari**. Si no han estat previstes, aquest tipus de fallades poden deixar el sistema totalment inoperant durant hores i fins i tot dies.

Tots els elements del maquinari poden deixar de funcionar en un moment determinat, no obstant això, cal identificar quins són més **crítics** per a la continuïtat del funcionament del nostre sistema.

Aquests són, bàsicament, les **fonts d'alimentació**, els **discos durs** i la **memòria**.

Solucions d'alta disponibilitat

Redundància en el maquinari (II) – **MTBF** –

Per poder dimensionar adequadament la solució que més ens convé, cal conèixer les dades de fiabilitat dels diferents components que formen un servidor. Normalment, els fabricants d'equips electrònics aporten entre altres dades tècniques l'anomenat **MTBF** (de l'anglès *mean time between failures*), que és el **temps mitjà entre fallades** expressat en hores.

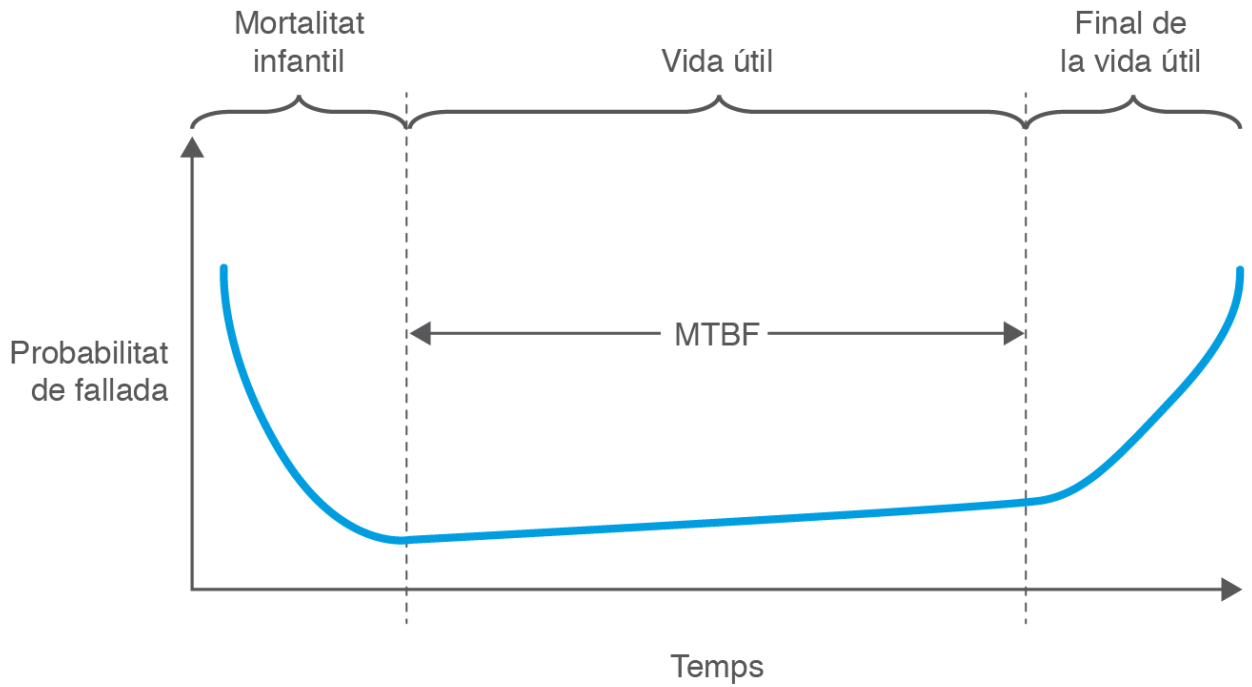
L'**MTBF** correspon exactament a la probabilitat inversa de fallada d'un sistema. A continuació s'indiquen alguns exemples d'MTBF:

- Disc dur: 10.000 – 20.000 hores
- Mòdem: 20.000 – 30.000 hores
- Ordinador personal: 1.000 – 5.000 hores
- Impressora: 2.000 – 4.000 hores

Alta disponibilitat

Solucions d'alta disponibilitat

Redundància en el maquinari (III) – **MTBF** –



Solucions d'alta disponibilitat

Redundància en el maquinari (IV) – **MTBF** –

Les tres etapes dels valors de l'MTBF:

- **Mortalitat infantil:** es considera que el primer any de vida d'un dispositiu és el període en què poden aparèixer més fallades. El motiu és clar: si hi ha hagut errors en la fabricació, males condiciones en l'emmagatzematge, defectes en els materials emprats per al muntatge o un tractament deficient en les manipulacions, és a l'inici del seu ús on aquests es manifestaran i causaran un mal funcionament.

- **Vida útil:** passat un any sense fallades, es considera que un dispositiu entra en la seva vida útil i la probabilitat que falli passa a ser l'**MTBF** indicat pel fabricant, sempre i quan el dispositiu treballi en les condicions necessàries de temperatura, humitat, vibracions… recomanades pel fabricant.

- **Final de la vida útil:** passats uns anys es considera que els components s'han degradat degut a l'ús, a la temperatura… i la probabilitat que fallin augmenta considerablement.

Solucions d'alta disponibilitat

Redundància en el maquinari (V) – *Exemple de càlcul de l'MTBF* –

Tenim un servidor un servidor que segons el fabricant té una **probabilitat de fallada de $1x10^{-4}$**. Per tant, el seu **MTBF** és: 1 / Probabilitat de fallada = 10.000 hores de vida útil. Aquest valor indica que estadísticament el servidor fallarà cada 416 dies.

L'empresa considera que aquest valor és massa baix i que necessita una disponibilitat més elevada. Per això decideix redundar el dispositiu completament i que dos servidors treballin en paral·lel. Per tant:

$$P(\text{sistema}) = P(\text{fallada servidor 1}) \cdot P(\text{fallada servidor 2}) = \mathbf{10^{-8}}$$

L'MTBF serà de 100.000.000 hores, amb la qual cosa la disponibilitat global del sistema ha augmentat de manera significativa.

Solucions d'alta disponibilitat

Redundància de servidors

Atès que en un servidor hi ha diversos components que poden deixar de funcionar i, en conseqüència, impedir al sistema oferir un nivell de servei adequat, s'acostuma a duplicar el servidor sencer. D'aquesta manera, sigui quin sigui el component que ha deixat de funcionar podem garantir un nivell de servei semblant al que s'ofereix en el servidor principal.

Es pot classificar la redundància de servidors en funció de la capacitat de resposta en cas de fallada:

- Redundància en **calent**
- Redundància **intermèdia**
- Redundància **freda**

Alta disponibilitat

Solucions d'alta disponibilitat

Redundància de servidors – *Redundància en calent* –

Es tracta de **dos servidors idèntics** sincronitzats que treballen en paral·lel, però dels quals **només un respon a les peticions del sistema**.

Disposen d'un **programari de supervisió mútua** i, en cas que el servidor que està responent en aquell moment entri en fallada, el servidor en espera prendrà el relleu en un temps suficient perquè el servei no es vegi afectat, habitualment de l'ordre de pocs mil·lisegons.

Alta disponibilitat

Solucions d'alta disponibilitat

Redundància de servidors – *Redundància intermèdia* –

Es tracta de dos servidors, un de **principal que respon a les peticions del sistema** i un de **secundari que no està sincronitzat en temps real**.

El servidor **secundari s'actualitza cada cert període de temps** prèviament establert, per exemple un cop al dia o un cop per setmana.

En cas de fallada es produeix una aturada en el servei, perquè el servidor secundari s'ha d'actualitzar amb les dades del sistema principal. Aquest tipus d'aturades poden durar entre pocs minuts i algunes hores.

Alta disponibilitat

Solucions d'alta disponibilitat

Redundància de servidors – *Redundància freda* –

Es tracta de dos servidors, un de **principal** que **respon a les peticions del sistema** i un de **secundari** amb característiques semblants, però que **no està operatiu**.

En cas de fallada s'hauria d'**iniciar** el servidor secundari, **instal·lar el programari actualitzat** i fer un **bolcat de** les **dades**.

L'activació d'un sistema d'aquest tipus acostuma a requerir algunes hores i fins i tot dies sencers de feina, en funció de les tasques que aquest hagi de dur a terme.