Activitat AS 03

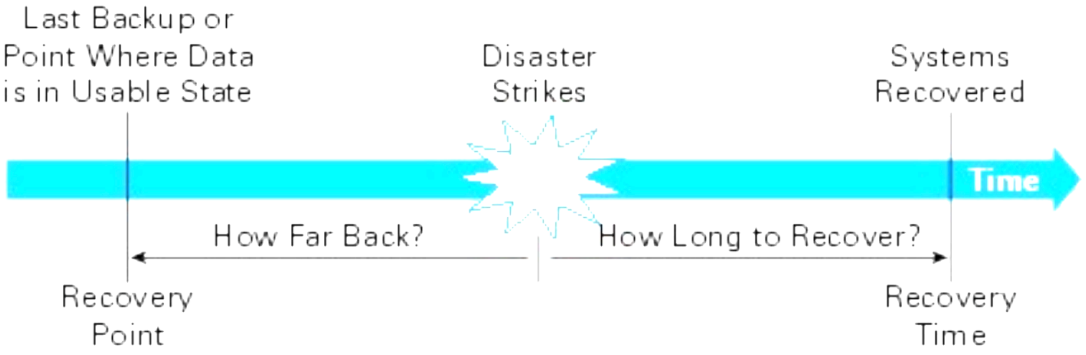
Data protection (classes 26 de febrer i 3 de març)

DATA LÍMIT DE LLIURAMENT: Dimarts 11 de Març, a mitjanit

NOM i COGNOMS: Sergio Shmyhelskyy Yaskevych

Descriu amb les teves paraules els següents conceptes:

a. Definició RPO i RTO, diferències amb RA i BIA.



- **RPO (Recovery Point Objective):** Defineix el màxim temps durant el qual es poden perdre dades en cas d'una fallada.

- **RTO (Recovery Time Objective):** Indica el temps màxim per restaurar el servei després d'una fallada.

- **RA (Risk Assessment)** i **BIA (Business Impact Analysis)**:
  - Risk Assessment és l'anàlisi dels riscos potencials, amenaces a la infraestructura (fallades de disc, atacs, desastres naturals …) i com es pot intentar prevenir-ho.

  - Business Impact Analysis determina l'impacte que pot tenir una interrupció en els processos crítics de negoci. És a dir, es centra en els sous que s'haurien de gastar per la discontinuïtat del negoci (generalment, els descrits per RA).

Mentre que RPO i RTO són mètriques específiques per a la recuperació, que indiquen quins són els punts màxims fins als que poden arribar els riscos, RA i BIA són processos més amplis que ajuden a identificar, avaluar i prioritzar els riscos i les seves conseqüències per a l'organització.

b. Defineix *hot spare disk* i la seva utilitat

Un *hot spare disk* és un disc de reserva (redundant) que és manté encès i connectat en el sistema, però sense participar com a emmagatzematge actiu. Quan falla un component clau es posa a funcionar.

Quan es detecta la fallada d'un disc actiu en una configuració RAID i provoca la degradació d'un grup d'emmagatzematge, el *hot spare disk* s'activa per substituir la unitat defectuosa, permetent que el grup d'emmagatzematge es recuperi en menys temps (reconstrucció automàtica d'informació) i proporcionar fiabilitat (minimitzant el temps d'inactivitat).

c. Problemes del backup: *frozen data*, temps de recuperació, perquè es fa en cintes majoritàriament?

Frozen data: Durant el procés de backup, les dades es poden "congelar" per assegurar que no es produeixin canvis mentre es fa la còpia, evitant així que es produeixin inconsistències entre còpies de seguretat, però això pot fer que la còpia no reflecteixi informació en temps real. S'obtindria una copia total de les dades que hi havien en l'instant que s'ha iniciat.

Temps de recuperació: És el període que passa desde que es comença a recuperar les dades amb els backups després d'haver tingut una fallada fins que es torni a tenir el sistema operatiu i que es pot seguir fent el treball normal. Es mesura amb RTO, en funció del volum de dades i la tecnologia usada, aquest temps hauria de ser mínim.

Els backups es fan en bona part en cintes magnètiques perquè son barats, en relació cost-GB-eficiència, amb la capacitat per emmagatzemar grans volums de dades i durabilitat. Tot i que les cintes tenen velocitats d'accés més lentes, ofereixen una **alta fiabilitat** per a l'arxiu a llarg termini i la recuperació de desastres (**portabilitat**).

d. Definició *full backup* i *synthetic backup*

Full backup: Còpia completa de totes les dades (no redundants) en un instant determinat, sense depende de còpies anteriors. Una alternativa a FB, ja que és bastant lent, es synthetic backup.

Synthetic backup: Còpia completa basada en l'últim backup complet amb tots els *incremental backup* (copies més petites que només guarden els canvis de de l'últim FB) que hi han hagut fins al moment, sense haver de realitzar una nova còpia completa de les dades originals.

S'usa per no interferir amb operacions actuals, ja que es fa "**out-of-server**", reduint així el temps i impacte en sistema.

e. Descriu la idea bàsica *de Shadow copy, snapshots i continuous data protection* (bàsica, un parell o tres de línies).

Shadow Copy o Business Continuity Volume (BCV): Crea còpies puntuals de les dades a uns altres discos fins a estar sincronitzades, mentre el sistema segueix en funcionament, permetent recuperar versions anteriors (que es pot transformar a un backup complet) sense interrompre el servei.

Fins que no es sincronitza del tot, es fan les escriptures tant com en els discos originals com en els *shadow copy* mentre es copia tot. Quan està tot sincronitzat (igual en totes dues bandes) es congelen les dades (*frozen data*).

Snapshots: Són captures que conserven l'estat i les dades d'un sistema en un moment determinat en que es fan. Consisteix en guardar els punters a disc del nostre sistema que apunten a regions de dades que han estat substituits, usant técnica COW (*copy-on-write*), d'aquesta forma si es vol recuperar senzillament s'ha d'accedir a través del punter. Són ràpids però amb poca durabilitat.

Continuous data protection (CPD) - Real-time backup: Cada canvi es desa automàticament (async - gairebé en temps real) a un servidor-backup separat, que normalment está ubicat a una altre xarxa (externa a la empresa). Si es desa a un servidor nostre d'empresa la informació es podría xifrar.
Es creen *journals* que contenen totes les operacions que s'han fet per si es vol fer un *roll-back* i tornar a un estat anterior.

Si vols que aquesta sigui una de les dues activitats AS que compten fins a 8 punts, aprofundeix en el següent tema (citant fonts i afegint els gràfics que consideris):

- Busqueu informació sobre *storage tiers* (veure la primera transparència d'aquest tema). Exemples i maneres de trobar un compromís entre la protecció i el cost. 3-4 pàgines seria un longitud normal.