

19. Egy ipari kutatásokkal foglalkozó vállalkozás szeretné növelni a cég adatbiztonságát.

Abban kérnek tanácsot, hogy hogyan tudnák az egyes kutatói munkaállomásokon, illetve a központi fájlserveren tárolt adatok biztonságát és helyreállíthatóságát garantálni minden körülmények között. Mutassa be ennek kapcsán az adatok biztonsági mentésének módjait a munkaállomásokon, illetve szerver környezetben! Biztonsági mentések mellett milyen más módon tudná növelni a szerverek adatbiztonságát? Mit javasolna a munkaállomások védelmére és a rajtuk tárolt adatok minél gyorsabb és egyszerűbb helyreállíthatóságára?

Kulcsszavak, fogalmak:

- biztonsági mentések fogalma, biztonsági mentésre használható eszközök
- biztonsági mentések típusai
- RAID, alapvető RAID szintek (0, 1, 0+1, 5)
- hardveres- és szoftveres RAID megvalósítások
- felhő alapú tárhely szolgáltatások (OneDrive, Google Drive, Tresorit, stb.), adatszinkronizáció
- vírusvédelem
- szünetmentes tápegységek

Az adatmentés a számítógépen tárolt információkról történő biztonsági másolat készítése, arra az esetre, mikor az eredeti forrásadatokat tartalmazó tároló megsérül.

Szoftveres és hardveres megoldások kombinációjaként megy végbe a folyamat. Nagyvállalati környezetben nem ritka az egymástól földrajzilag távol lévő irodák közti adatkommunikáció, valamint a távoli szerverekre történő adatmentés. Ehhez nagyszámú szoftver áll rendelkezésre. Az adatmentő szoftverek közül a legjobb megoldás a hardverfüggetlen mentőszoftver. Ez azért fontos, mert ha működésképtelenné válik egy hardver és nem tudunk ugyanolyat vagy hasonlót beszerezni, más hardveren is vissza tudjuk állítani az adatainkat.

A mentés többféle módszer szerint történhet:

Teljes mentés

Növekményes mentés

Differenciális mentés

Teljes mentés: Ha mindig teljes mentést készítünk, az összes közül a legtöbb tárhelyet igénylő megoldás, azonban a visszaállítás a lehető legegyszerűbb, illetve minden egyéb mentési rendnek ez az alapja.

Differenciális (különbségi mentés)

Mindig az utolsó teljes mentés óta változott adatokat mentjük. Ez azzal jár, hogy a differenciális mentés a teljes mentést követően folyamatosan növekszik. A visszaállításhoz az utolsó teljes és utolsó differenciális mentésre van szükség.

Növekményes mentés: A folyamat itt is egy teljes mentéssel kezdődik, utána mindig az utolsó mentés óta történt változásokat mentjük. A teljes visszaállításhoz az utolsó teljes mentésre és az összes inkrementális mentésre szükség van. Ezzel a módszerrel az utolsó teljes mentésig visszamenőleg bármely korábbi állapot is visszaállítható.

Adathordozó

A használt tároló modelltől függetlenül az adatokat tárolni kell bizonyos adathordozóra.

Mágneses szalag

A mágneses szalag már régóta a leggyakrabban használt adathordozó az ömlesztett adattárolás, biztonsági mentés, archiválás és adatcsere számára. szalag általában nagyobb nagyságrendű jobb kapacitás-ár arányt mutatott a merevlemezhez képest, de a közelmúltban a szalag és a merevlemez arányai sokkal közelebb kerültek. Számos formátum létezik, amelyek közül sok a tulajdonos vagy egyes piacokra jellemző, például nagyszámítógépek vagy a személyi számítógép egy bizonyos márkája. A szalag egy soros hozzáférési közeg, így bár a hozzáférési idők rossz lehet, az adatok folyamatos írása vagy olvasása ténylegesen nagyon gyors lehet. Néhány új szalagos meghajtó még gyorsabb, mint a modern merevlemezek.

Merevlemez

A merevlemez kapacitás-ár aránya sok év alatt gyorsan javult. Ezáltal a mágneses szalaggal versenyképesebbé válik, mint ömlesztett adathordozó. A merevlemez-tárolás legfontosabb előnyei az alacsony hozzáférési idő, a rendelkezésre állás, a kapacitás és a könnyű használat. A külső lemezeket helyi interfészek, például SCSI, USB, FireWire vagy eSATA, vagy hosszabb távú technológiák, például Ethernet, iSCSI vagy Fibre Channel segítségével lehet csatlakoztatni. Egyes lemezalapú biztonsági rendszerek, például a virtuális szalagkönyvtárak támogatják az adatok deduplikációját, ami drámaian csökkentheti a napi és heti biztonsági mentési adatok által felhasznált lemez tárolókapacitását. A merevlemez-mentések legfőbb hátránya, hogy könnyen károsodnak, különösen a szállítás során (például a helyszíni biztonsági mentéseknél), és hogy évek közötti stabilitásuk viszonylag ismeretlen.

Optikai tárolás

A rögzíthető CD-ket, DVD-ket és Blu-ray lemezeket általában a személyi számítógépekkel használják, és általában alacsony a médiaköltség. Mindazonáltal ezeknek és más optikai lemezek kapacitása és sebessége jellemzően kisebb nagyságrendű, mint a merevlemez vagy a szalag. Sok optikai lemezformátum WORM típusú, ami archiválásra használható, mivel az adatok nem módosíthatók. Az automatikus váltó vagy a zenegép használatával az optikai lemezek megvalósíthatók a nagyobb méretű biztonsági rendszerek számára. Egyes optikai tárolórendszerek lehetővé teszik a katalógusban tárolt adatok mentését emberi érintkezés nélkül a lemezekkel, ami lehetővé teszi a hosszabb adatintegritást.

Szilárd állapotú tárolás

Más néven flash memória, hüvelykujj meghajtók, USB flash meghajtók, CompactFlash, SmartMedia, Memory Stick, Secure Digital kártyák stb. Ezek a készülékek viszonylag drágák alacsony kapacitásukhoz és a merevlemezekhez képest, de nagyon kényelmesek és a biztonsági mentéshez viszonylag alacsony adatmennyiségek. A szilárdtest-meghajtó nem tartalmaz semmiféle mozgatható részt, ellentétben a mágneses meghajtókészülékével, így kevésbé érzékeny a fizikai károsodásra, és hatalmas átviteli teljesítménye 500Mbit/s–6Gbit/s. Az SSD-k által kínált kapacitás tovább növekszik, és az árak egyre alacsonyabbá válnak.

Távoli mentési szolgáltatás

Amint a széles sávú internet-hozzáférés egyre szélesebb körben elterjedt, a távoli mentési szolgáltatások egyre népszerűbbek. Az interneten távoli helyre történő mentés védelmet nyújt a legrosszabb forgatókönyveknek, például tüzekkel, áradásokkal vagy földrengésekkel, amelyek minden más biztonsági mentést elpusztítanak a közvetlen környezetben. Van azonban számos hátránya a távoli mentési szolgáltatásoknak. Először is, az internetkapcsolatok általában lassabbak, mint a helyi adattárolók. A lakossági széles sávú szolgáltatások különösen problémásak, mivel a rutin biztonsági mentéseknek olyan upstream linket kell használnia, amely általában sokkal lassabb, mint a downstream link, amelyet csak alkalmanként használnak a fájl biztonsági másolatának lekéréséhez. Ez általában korlátozza az ilyen szolgáltatások viszonylag kis értékű, nagy értékű adatainak használatát. Másodszor, a felhasználóknak meg kell bízniuk egy harmadik féltől származó szolgáltatót, hogy megőrizze adataik adatainak biztonságát és integritását, bár a titkosságot az adatok titkosítása előtt biztosíthatja a biztonsági szolgálatnak a titkosítási kulcs segítségével történő átvitelét megelőzően. Végül a biztonsági mentési szolgáltatásnak magának kell alkalmaznia a fenti módszerek valamelyikét, így ez a hagyományos biztonsági mentések összetettebb módjának tekinthető.

A RAID (angolul Redundant Array of Inexpensive Disks vagy Redundant Array of Independent Disks^{[1][2]}) tárolási technológia, mely segítségével az adatok elosztása vagy replikálása több fizikailag független merevlemezen, egy logikai lemez létrehozásával lehetséges. Minden RAID szint alapján véve vagy az adatbiztonság növelését vagy az adatátviteli sebesség növelését szolgálja.

RAID szintek

A RAID-ben eredetileg 5 szintet definiáltak (RAID 1-től RAID 5-ig). Az egyes szintek nem a fejlődési, illetve minőségi sorrendet tükrözik, hanem egyszerűen a különböző megoldásokat. A kezdeti 5 szinthez később hozzávették a RAID 6-ot. RAID 0-ként szokták említeni azt a változatot, ahol a lemezeket összefűzzük, azaz redundancia nélkül kapcsoljuk össze. Ezekon kívül használják még több RAID tömb egymásra építését is, a legelterjedtebb a RAID 10 (vagy RAID 1+0), RAID 01 (vagy RAID 0+1), illetve a RAID 50 (vagy RAID 5+0). A RAID alapötlete a lemezegységek csíkokra (stripes) bontása. Ezek a csíkok azonban nem azonosak a lemez fizikai sávjaival (tracks), amit az angol és magyar elnevezés különbözősége is jelez.

RAID 0

A RAID 0 az egyes lemezek egyszerű összefűzését jelenti, viszont semmilyen redundanciát nem ad, így nem biztosít hibátűrést, azaz egyetlen meghajtó meghibásodása az egész tömb hibáját okozza. Mind az írási, mind az olvasási műveletek párhuzamosítva történnek, ideális esetben a sebesség az egyes lemezek sebességének összege lesz, így a módszer a RAID szintek közül a legjobb teljesítményt nyújtja (a többi módszernél a redundancia kezelése lassítja a rendszert). A megoldás lehetővé teszi

különböző kapacitású lemezek összekapcsolását is, viszont a nagyobb kapacitású lemezeken is csak a tömb legkisebb kapacitású lemezének méretét lehet használni (tehát egy 120 GB és egy 100 GB méretű lemez összefűzésekor mindössze egy 200 GB-os logikai meghajtót fogunk kapni, a 120 GB-os lemezen 20 GB szabad terület marad, amit más célokra természetesen felhasználhatunk). A RAID 0 főleg olyan helyeken alkalmazható, ahol nem szempont az adatbiztonság vagy kevés merevlemez csatlakozhat fel az operációs rendszer korlátozása miatt. (Például a régebbi Microsoft Windows rendszerek esetében összesen 26 meghajtó betűjelet tesznek elérhetővé, ezzel 24 eszközre korlátozva a partíciók számát. Az újabb rendszerek, mint a Windows 2000 Professional és az ezt követő Windowsok, valamint a Unix rendszerek lehetőséget adnak a partíciók könyvtárként való felcsatlakozására.) A másik pozitív tulajdonsága viszont továbbra is csábító lehet olyan, kifejezetten csak játékokra épített rendszereknél, ahol ezzel tetemes teljesítménynövekedést érhetünk el. Ilyen célú alkalmazásra mégsem túl ajánlott, mivel az egyszer már összekapcsolt diszkek különálló alkalmazása csak újraszervezés után, a teljes adattartalom eltávolításával és újraformázással lehetséges.

RAID 1

A RAID 1 eljárás alapja az adatok tükrözése (disk mirroring), azaz az információk egyidejű tárolása a tömb minden elemén. A kapott logikai lemez a tömb legkisebb elemével lesz egyenlő méretű. Az adatok olvasása párhuzamosan történik a diszkekről, felgyorsítván az olvasás sebességét; az írás normál sebességgel, párhuzamosan történik a meghajtókon. Az eljárás igen jó hibavédelmet biztosít, bármely meghajtó meghibásodása esetén folytatódhat a működés. A RAID 1 önmagában nem használja a csíkokra bontás módszerét.

RAID 2

A RAID 2 használja a csíkokra bontás módszerét, emellett egyes meghajtókat hibajavító kód (ECC: Error Correcting Code) tárolására tartanak fenn. A hibajavító kód lényege, hogy az adatbitekkel valamilyen matematikai művelet segítségével redundáns biteket képeznek. A használt eljárástól függően a kapott kód akár több bithiba észlelésére, illetve javítására (ez utóbbi persze több redundanciát igényel) alkalmas. A védelem ára a megnövekedett adatmennyiség. Ezen meghajtók egy-egy csíkjában a különböző lemezekon azonos pozícióban elhelyezkedő csíkokból képzett hibajavító kódot tárolnak. A módszer esetleges lemezhiba esetén képes annak detektálására, illetve kijavítására. Manapság nem használják, mivel a SCSI meghajtókban már minden egyes szektorban az adott szektorhoz tartozó ECC is eltárolódik.

RAID 3

A RAID 3 felépítése hasonlít a RAID 2-re, viszont nem a teljes hibajavító kód, hanem csak egy lemeznyi paritásinformáció tárolódik. Egy adott paritáscsík a különböző lemezekon azonos pozícióban elhelyezkedő csíkokból XOR művelet segítségével kapható meg. A rendszerben egy meghajtó kiesése nem okoz problémát, mivel a rajta lévő információ a többi meghajtó (a paritást tároló meghajtót is beleértve) XOR-aként megkapható. Az alapvető különbség a RAID 2-ben alkalmazott hibajavító kóddal szemben, hogy itt feltesszük, hogy a meghajtó meghibásodását valamilyen módon (például többszöri sikertelen olvasás hatására) észleljük, majd a meghibásodott diszken lévő információt a többi diszken lévő adatok segítségével állítjuk elő. A RAID 2 a diszkehibák ellen is védelmet nyújt, például egyes bájtok megsérülése esetén. (Vegyük észre, hogy csak az XOR-os paritásbit technikát használva az egyik meghajtón egy adott bájt megsérülése esetén csak azt vennénk észre, hogy a különböző meghajtókon az azonos csíkba tartozó részek XOR-a nem nullát adna, de nem tudnánk sem azt, hogy melyik meghajtón van a hiba, sem azt, hogy hogyan javítsuk ki. Ezért van szükség a szektoronkénti hibajavító kód alkalmazására.)

A RAID 3-nál kisméretű csíkokat definiálnak, így az egyes fájlok olvasása és írása párhuzamosan történhet az egyes meghajtókon, viszont a módszer nem támogatja egyszerre több kérés párhuzamos kiszolgálását (single-user mode). (Természetesen a paritáscsíkot minden egyes íráskor módosítani kell, amihez szükséges a korábbi tartalom kiolvasása. Viszont például fájltranszfer esetén, pont a kisméretű csíkok miatt, az azonos pozícióban lévő csíkokat általában az összes diszken felülírják, így ez esetben a probléma kevésbé jelentkezik.)

RAID 4

A RAID 4 felépítése a RAID 3-mal megegyezik. Az egyetlen különbség, hogy itt nagyméretű csíkokat definiálnak, így egy rekord egy meghajtón helyezkedik el, lehetővé téve egyszerre több (különböző meghajtókon elhelyezkedő) rekord párhuzamos írását, illetve olvasását (multi-user mode). Problémát okoz viszont, hogy a paritás-meghajtó adott csíkját minden egyes íráskor frissíteni kell (plusz egy olvasás és írás), aminek következtében párhuzamos íráskor a paritás-meghajtó a rendszer szűk keresztmetszetévé válik. Ezenkívül valamely meghajtó kiesése esetén a rendszer olvasási teljesítménye is lecsökken, a paritás-meghajtó jelentette szűk keresztmetszet miatt.

RAID 5

A RAID 5 a paritás információt nem egy kitüntetett meghajtón, hanem „körbeforgó paritás” (rotating parity) használatával, egyenletesen az összes meghajtón elosztva tárolja, kiküszöbölve a paritás-meghajtó jelentette szűk keresztmetszetet. Minimális meghajtószám: 3. Mind az írási, mind az olvasási műveletek párhuzamosan végezhetőek. Egy meghajtó meghibásodása esetén az adatok sértetlenül visszaolvashatóak, a hibás meghajtó adatait a vezérlő a többi meghajtóról ki tudja számolni. A csíkméret változtatható; kis méretű csíkok esetén a RAID 3-hoz hasonló működést, míg nagy méretű csíkok alkalmazása esetén a RAID 4-hez hasonló működést kapunk. A hibás meghajtót ajánlott azonnal cserélni, mert két meghajtó meghibásodása esetén az adatok elvesznek! A tárolható adatmennyiség "a legkisebb kapacitású meghajtón tárolható adatmennyiség" * ("meghajtók száma" - 1) lesz. (Pl. 4 db egyenként 1 TB -os HDD RAID 5-be fűzésének eredményeként egy 3 TB kapacitású logikai meghajtót látunk.) Az írási sebességnél fontos figyelembe venni a paritás adatok előállítására szükséges számítási kapacitás igényt! Szoftveres megoldásnál ez jelentős processzorterhelést, illetve az írási sebesség csökkenését eredményezheti, ezért ajánlott a hardveres megoldás, ahol a célhardver látja el ezeket a feladatokat. A RAID 5 vezérlők a hibás meghajtó helyére betett új, üres meghajtót automatikusan fel tudják tölteni az eredeti adatokkal. A hibás meghajtó egy-egy blokkját a következőképpen lehet visszaolvasni: $A_h = (A_{j1} \text{ XOR } A_{j2}) \text{ XOR } A_{j3}$, ahol A_h : a fizikailag hibás meghajtó része és A_{j1} , A_{j2} , A_{j3} : a jó meghajtó része. Az "olvasási sebesség" = "A leglassabb meghajtó olvasási sebessége" * ("Meghajtók száma" - 1) A tömb egyetlen meghajtójáról nem állítható vissza a teljes adattartalom, viszont egy-egy adatblokknyi igen. Mivel akár ez is tartalmazhat értékes információt, így a már nem használt vagy hibás adathordozót érdemes megsemmisíteni.

RAID 6

A RAID 6 tekinthető a RAID 5 kibővítésének. Itt nemcsak soronként, hanem oszloponként is kiszámítják a paritást. A módszer segítségével kétszeres meghajtómeghibásodás is kiküszöbölhetővé válik. A paritáscsíkokat itt is az egyes meghajtók között, egyenletesen elosztva tárolják, de ezek természetesen kétszer annyi helyet foglalnak el, mint a RAID 5 esetében.

RAID 0+1 vagy RAID 01

Ez egy olyan hibrid megoldás, amelyben a RAID 0 által hordozott sebességet a RAID 1-et jellemző biztonsággal ötvözzhetjük. Hátránya, hogy minimálisan 4 eszközre van szükségünk, melyekből 1-1-et összefűzve, majd páronként tükrözve építhetjük fel a tömbünket, ezért a teljes kinyerhető kapacitásnak mindössze a felét tudjuk használni. Mivel a tükrözés (RAID 1) a két összefűzött (RAID 0) tömbre épül, ezért egy lemez meghibásodása esetén az egyik összefűzött tömb mindenképp kiesik, így a tükrözés is megszűnik.

RAID 1+0 vagy RAID 10

Hasonlít a RAID 01 megoldáshoz, annyi különbséggel, hogy itt a lemezeket először tükrözzük, majd a kapott tömböket fűzzük össze. Ez biztonság szempontjából jobb megoldás, mint a RAID 01, mivel egy diszk kiesése csak az adott tükrözött tömböt érinti, a rá épült RAID 0-t nem; sebességben pedig megegyezik vele.

Mi az a szoftveres RAID?

A szoftveres RAID a RAID egy olyan típusa, amely szoftvert használ a több merevlemezen tárolt adattárolás kezelésére. Általában az operációs rendszeren keresztül valósul meg, bár van néhány kivétel. A szoftveres RAID esetén a CPU felelős az adattárolás kezeléséért, ami befolyásolhatja a teljesítményt.

Mi az a hardveres RAID?

A hardveres RAID ezzel szemben egy dedikált hardvervezérlőt használ az adattárolás kezelésére. Ez tehermentesíti a CPU-t, ami javíthatja a teljesítményt. A hardveres RAID általában fejlettebb szolgáltatásokat és rugalmasságot kínál, mint a szoftveres RAID.

Szoftveres RAID vs hardveres RAID: Főbb különbségek

Most, hogy áttekintettük az egyes RAID-típusok alapjait, nézzük meg alaposabban a szoftveres RAID és a hardveres RAID közötti fő különbségeket:

- **Teljesítmény:** Mint említettük, szoftveres RAID esetén a CPU felelős az adattárolás kezeléséért. Ez befolyásolhatja a teljesítményt, különösen a meghajtók számának növekedésével. A hardveres RAID viszont egy dedikált hardvervezérlőt használ, amely javíthatja a teljesítményt.
- **Jellemzők:** A hardveres RAID jellemzően fejlettebb szolgáltatásokat kínál, mint a szoftveres RAID, például a hot tartalék támogatást és több RAID-tömb létrehozásának lehetőségét. Ez nagyobb rugalmasságot biztosíthat a tárhely konfigurálásában.
- **Költség:** A hardveres RAID egyik fő hátránya a költség. A dedikált hardvervezérlő drága lehet, és maguknak a meghajtóknak a költségeit is figyelembe kell venni. A szoftveres RAID segítségével alacsonyabb költségű meghajtókat használhat, mivel a CPU végzi a munkát.
- **Beállítás:** A hardveres RAID másik hátránya, hogy bonyolultabb lehet a beállítása. Telepítenie kell a dedikált hardvervezérlőt, és konfigurálnia kell a meghajtókat. A szoftveres RAID esetén a beállítás általában sokkal egyszerűbb, mivel mindez az operációs rendszeren keresztül történik.

A **felhőalapú számítástechnika** (angolul „cloud computing”) a számítástechnika egyik ágazata. Többféle felhőalapú szolgáltatást különböztethetünk meg, a közös bennük az, hogy a szolgáltatásokat nem egy meghatározott hardvereszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, annak üzemeltetési részleteit a felhasználótól elrejtve. A szolgáltatásokat a felhasználók hálózaton keresztül érhetik el, publikus felhő esetében az interneten keresztül, privát felhő esetében a helyi hálózaton vagy ugyancsak az interneten.

A felhőalapú szolgáltatások három fő csoportja

- Szoftverszolgáltatás (**Software as a Service**)
A szoftvert magát nyújtja szolgáltatásként. Ezeket az alkalmazásokat általában http protokollon keresztül, egy böngészővel lehet használni. Példa: Google Docs, netsuite.
- Platform szolgáltatás (**Platform as a Service**)
Az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja, terheléelosztással és feladatátvétellel, kezelőfelülettel, ezek rendszeres biztonsági frissítésével. Példa: Google App Engine, OpenShift.
- Infrastruktúra szolgáltatás (**Infrastructure as a Service**)
Virtuális hardvert (szervert, blokk-tárhelyet, hálózati kapcsolatot, számítási kapacitást) szolgáltat. Példa: Amazon EC2, Google Compute Engine

Hozzáférhetőség alapján:

- Publikus felhő
Publikus felhő esetén egy szolgáltató a saját eszközállományával (tárhely, hálózat, számítási kapacitás) szolgálja ki ügyfelei szerverigényeit. Publikus felhők esetén különösen fontos a különböző ügyfelek izolálása.
- Privát felhő
Saját vagy bérelt erőforrásokon lehet saját felhőt is építeni. Ez megoldást jelent a publikus felhők problémáira, viszont az üzemeltetésről a privát felhő tulajdonosának kell gondoskodnia.^{[4][5]} Példák privátfelhő-szoftverekre: VMware vSphere, oVirt, CloudStack, OpenNebula
- Hibrid felhő
Privát és publikus felhők kombinációja. A hibrid felhő egyesíti a lokális (on-premise) adatközpont, a privát felhő és a publikus felhő elemeit oly módon, hogy ezek a különböző komponensek kommunikálhassanak egymással. A párhuzamosan működtetett a privát felhő és publikus felhő még nem jelent automatikusan hibrid felhőt. Csak abban az esetben beszélhetünk hibrid felhőről, ha az adatok következetes, szinkronizált módon áramolhatnak a különböző felhőmodellek között.^[6]
- Közösségi felhő
Hasonló törvényi szabályozás alá eső szervezetek hozzák létre, például amerikai költségvetési intézményeknek van ilyen.^[7]

Egyéb kategóriák

- Tárhelyszolgáltatás (Storage as a Service)
A tárhelyet adja mint szolgáltatást. Például: Amazon S3, iCloud.
Ide sorolhatjuk a biztonsági mentéseket és szinkronizációs szolgáltatásokat is.

Vírusvédelem.....

A **szünetmentes tápegység** (angolul: *Uninterruptible Power Supply*, röviden: UPS) olyan eszköz, mely villamos energiát biztosít számítógépeknek és egyéb berendezéseknek, akkor is, ha a villamos hálózaton bármilyen ok miatt megszűnik a készülék működéséhez szükséges tápfeszültség

Áthidalási idő:

A szünetmentes tápegységek egyik legfontosabb jellemző adata. Megadja, hogy névleges terhelés esetén mennyi ideig képes a berendezés a rákapcsolt fogyasztókat villamos energiával ellátni. Ez az idő felépítéstől függően néhány 10 másodperctől a néhány óráig terjed. A ténylegesen tapasztalható áthidalási időt befolyásolja a táplált fogyasztók tényleges energia igénye, és az energiatároló pillanatnyi állapota (pl. öregedés miatti kapacitás csökkenés).