Тема 21. Защита и възстановяване от сривове

Аварийно захранване
Архивиране на данните
  Какво трябва да се архивира?
  Кога да се архивира?
  С каква програма да се архивира?
  На какъв носител да се архивира?
  Кой да отговаря за извършване на архивирането?
Отказоустойчивост
  RAID 0 – Лентов набор (Disk Stripping)
  RAID 1 – Огледални дискове (Disk Mirroring)
  RAID 3 – Лентов набор с големи блокове (Disk Stripping with Large Blocks)
  RAID 5 – Лентов масив с контрол по четност (Stripping with Parity)
  RAID 10 – Огледални дискови масиви (Mirrored Disk Arrays)
Въпроси

При планиране на мрежовата сигурност трябва да се има предвид и възможността за загуба на информация поради природни бедствия, хардуерни повреди и технически грешки. Затова е необходимо да се планират мероприятия за защита на данните и възстановяване от сривове.

Съществуват три начина за предотвратяване на загубите на информация:

- Аварийно захранване
- Архивиране на данните
- Отказоустойчивост

Аварийно захранване

Гръмотевичните бури и пренапреженията, които могат да възникнат в електрическата мрежа могат да доведат не само до загуба на данни, но и до повреди в хардуера. Най-евтиният начин за предпазване от пренапрежения е чрез поставяне на ***предпазител от пренапрежение***.

Предпазителят от пренапрежение е защитно устройство, което ограничава повишаванията на напрежението. Желателно е всеки компютър в мрежата да бъде снабден с такова устройство. Той предпазва от възникващите пренапрежения, но не осигурява енергоподаване при спиране на захранването.

По-добрият вариант е използването на непрекъсваемо устройство – **UPS** (Uninterruptible power supply). *UPS е автоматизирано външно захранващо устройство, което осигурява електроенергия за компютрите и други устройства, когато основното електрозахранване спре*. UPS системите осигуряват:

- захранване за компютрите и сървъра за кратко време;
- безопасно изключване на системата.

UPS устройството се поставя между компютърната система и основния източник на електроенергия. Чрез един UPS обикновено могат да се захранят няколко компютъра или други устройства. При изключване на основното електрозахранване UPS уведомява потребителите в мрежата (напр. чрез звуков сигнал) за възникналия проблем. Потребителите имат възможност да съхранят данните, с които са работили и да изключат безопасно системата.

Smart UPS системите работят в режим он-лайн. Те генерират непрекъснато синусоидално 220V 50Hz напрежение, като едновременно черпят и зареждат акумулаторите си. Те осигуряват галванична развързаност от захранващата мрежа. При пренапрежение UPS системите пропускат само част от пиковото напрежение, обикновено с коефициент на затихване 1/1000 или 1/2000.

Back UPS системите работят в режим stand-by. При наличие на захранване, те осигуряват директна връзка на консуматорите към захранващата мрежа. Когато се прекъсне електрозахранването UPS автоматично го замества.

При избор на UPS трябва да се съобразим със следните въпроси:

- Колко системи, с каква обща мощност ще трябва да захранва UPS устройството?
- Предлага ли се софтуер, осигуряващ възможност за уведомяване на потребителите и мрежовия администратор при прекъсване на захранването? Позволява ли софтуера безопасно изключване на захранваните системи?
- За колко системи е защитата за безопасно изключване? Ако са включени няколко компютъра към UPS, поддържа ли се изключване на всички компютри?
- Ефективна ли е защитата срещу токови удари?
- Има ли допълнителна защита за пренапрежения към мрежовата карта?
- Каква е продължителността на живот на батерията?

Мощността на UPS се измерва във волт-ампери (VA, пълна мощност). Мощността на консуматорите се измерва във ватове (W, активна мощност). Електрическите товари потребяват както активна, така и реактивна енергия. За изчисляване на необходимата пълна мощност на UPS система, захранваща компютърни системи се използва коефициент на мощността. Представлява отношение на активната мощност (W) към реактивната мощност (VA), потребявана от товара. За компютърни системи с импулсен захранващ блок този коефициент е над 0.7 .

Как да се определи необходимата мощност на UPS? Например, ако мощността на UPS устройството е 1000VA, при коефициент 0.7 той може да захранва консуматори с мощност до 700W. По-правилно е при избор на UPS да се остави резерв на мощността и за коефициента да се избере стойност 0.6, така 1000VA UPS може да захрани консуматори с мощност до 600W.

UPS защитават компютрите и данните в тях при отпадане на захранването, но те не осигуряват възможност за продължително захранване. За целта непрекъсваемите захранващи системи могат да се комбинират с ***генератор на напрежение***.

Интернет ресурси за UPS:
http://comexgroup.com/technologies/_power/tripp-lite.htm
http://www.computerworld.bg/?call=USE~home;&page=paper&n=13707&pn=1

Архивиране на данните

Независимо от положените усилия за защита на данните, винаги съществува възможност за тяхната загуба. Причините за загуба на данни са многобройни. Ето най-честите от тях:

1. Повреда на твърдия диск
2. Повреда на инсталацията на операционната система
3. Изгубване, изтриване
4. Вирусна атака
5. Кражба
6. Природни бедствия

За да се предотврати загубата на данните е необходимо те да бъдат архивирани. Това е процес на създаване на копие на данните, обикновено на външен носител. Има различни програмни решения за архивиране, предлагани от операционната система или като самостоятелни продукти.

Всяка организация трябва да си създаде политика по архивирането. При архивиране на данните трябва да се отговори на следните въпроси:

Какво трябва да се архивира?

Трябва да се създаде приоритет на различните типове документи, бази данни, файлове, които следва да се съхраняват. Очевидното решение – да се архивира всичко –е най-добро, но очевидно изисква най-много време и физически носители. Операционната система, инсталираните програмни продукти могат да се възстановят. Данните и документите, които потребителите създават са резултат на много време и усилия. Творческата работа, финансовата информация имат най-голям приоритет.

За да се архивира успешно, процесът на архивиране трябва се автоматизира. Това е невъзможно, ако данните са разпръснати по персоналните компютри на служителите. Политиката по архивирането трябва да реши: Къде да се съхраняват фирмените документи? Кои потребители имат право локално да съхраняват своите файлове и документи? Трябва да се създаде административна рамка, осигуряваща централизиране на документите на един компютър – сървър. Така при срив на компютърна система, когато тя не съдържа данни на служителя, тя може да се замени с друга, съдържаща идентичен инсталиран софтуер.

Кога да се архивира?

Архивирането трябва да се извършва периодично. Времето за архивиране зависи от това колко данни може да си позволим да загубим: за 1 ден, 1 седмица, 1 месец? Архивирането може да се извършва автоматично по график след работно време.

Има три типа архивиране:

- Пълно архивиране – съхраняват се всички данни;
- Диференциално архивиране – съхраняват се данните, променени след пълното архивиране;
- Инкрементално архивиране – архивират се данните, променени след последното архивиране (не след пълно архивиране).

Пълното архивиране изисква най-много време и дисково пространство, но е най-лесно за изпълнение. За възстановяване на състоянието след диференциално архивиране е необходимо първо да се възстанови последният пълен архив и върху него да се възстанови диференциалния архив. Аналогично, за да се възстанови системата чрез инкрементален архив е необходимо да се възстанови пълния архив, след него последователно да се разархивират всички инкрементални архиви. Разбира се, всяка програма за архивиране позволява преглед на съдържанието на архивите и възстановяване на файл, файлове или папки по избор на потребителя.

С каква програма да се архивира?

Системите за архивиране, които са част от операционната система (ОС), например ntbackup за Windows, предлагат пълно архивиране. Проблемът при използването на такъв архив, е че трябва ОС да е стабилна, работоспособна. Това означава, че след срив трябва първо да се инсталира ново копие на ОС и след това да се разархивират данните, за да се възстанови системата към точката на архивиране.

Съществуват редица програми, които създават снимка (snapshot) на системата. Например Norton Ghost може да създаде снимка – архив на цял диск или на дял (partition) на твърдия диск. Това може да стане, когато ОС е неактивна. Трябва да се извърши първоначално зареждане на MS DOS операционна система например от компакт-диск (или дискета, флаш-памет) и след това да се направи архива. Това означава, че архивирането не може да стане автоматично, необходимо е системата да бъде спряна, за да се архивира. Предимството на архив ‘snapshot’ е, че най-лесно и бързо се възстановява. След рестартиране имаме състоянието на системата към момента на създаване на архива. Ако разархивирането се прави на същата компютърна система, не са необходими никакви допълнителни усилия за нейното възстановяване.

Добро решение е да се правят различни архиви с различни програмни продукти. Може веднъж в месеца да се прави архив – snapshot, всяка седмица по разписание – пълен архив и всяка вечер – инкрементален архив. На архивирането на базите данни трябва да се обърне особено внимание. Ако не е достатъчно архивиране веднъж на ден в извънработно време, ще се наложи да се архивира базата данни в момент, в който в нея се извършват операции. Системите за управление на бази данни (СУБД) като Oracle, предлагат инструмент за архивиране, позволяващ on-line архивиране – създаване на сполучлива снимка на работещата система.

На какъв носител да се архивира?

Програмните продукти за архивиране създават архив обикновено на твърдия диск. Те позволяват запис на архива и на външен носител, но проблемът е, че размерът на твърдите дискове превишава в пъти размера на най-големия носител (най-голямата магнитна лента към момента (2008 г.) е SLR – до 70GB некомпресирани). За да има пълно архивно копие, то трябва

да се съхранява извън предприятието/организацията. За това трябва да се съхрани на външен носител.

Най-често използваните носители са DVD-R, DVD+R дискове. Техният капацитет е 4.5GB. Следващата еволюционна стъпка в развитието на DVD устройствата са Blue Ray дисковете, с размер на CD/DVD, те позволяват до 25GB едностранен запис и до 50GB двустранен запис. Разбира се, като всяка нова технология, цената за архивиране на 1GB информация е в пъти по-висока в сравнение с цената на DVD дисковете.

В много организации, размерът на твърдите дискове достигна терабайт (1TB). Записът на цялата тази информация на външни носители е трудно осъществимо. Очевидното решение е да се извършва архивиране на друг твърд диск, за предпочитане външен, с USB или LAN интерфейс. Дори при най-високите скорости, архивирането ще отнеме денонощие и ще изисква през това време системата да е недостъпна за потребителите си.

Всички програми за архивиране извършват компресиране на информацията за икономия на дисково пространство и носители. Средно компресията е около 50%. Създадените архиви на външни носители трябва да се съхраняват в определено за целта помещение. Тъй като те съдържат особено важна информация, която трябва да си остане фирмена тайна, тяхното съдържание трябва да се криптира. Политиката за архивирането трябва да реши къде да се съхраняват архивите, как да се криптират и как да се съхраняват криптографските ключове. Добро решение е да се съхраняват архивите в банков сейф. Така отпада необходимостта от криптиране и защита на архивите от унищожение. Съхраняването на архива в предприятието/организацията, особено в сървърското помещение, не е добра идея. След бедствие като пожар, наводнение, кражба и други могат да бъдат загубени, както компютърните системи, така и архивите.

Кой да отговаря за извършване на архивирането?

Добре е да има определен служител, който да отговаря за архивирането на данните. Освен архивиране, той трябва периодично да проверява целостта на системата за архивиране чрез тестово разархивиране на данните. Грешка в процедурата за архивиране може да се открие късно – едва след като данните бъдат загубени завинаги.

Трябва да се създаде план за възстановяване след загуба на компютърни системи и данни. Да се предвиди закупуването на нови компютри, преинсталиране на програмните продукти. Част от използваните лицензни програмни продукти се инсталират само от дистрибуторите си. Трябва да се подържа контакт с тях, за да може да се възстанови специфичното приложение и неговите данни. Трябва да се предвиди заместник на служителя, отговорен за архивирането – може да е друг достатъчно квалифициран служител или да се наеме външна фирма.

Отказоустойчивост

Системите за отказоустойчивост предпазват данните от загуба чрез дублиране на самата хардуерна система. Например, много важни сървъри притежават по два захранващи блока, при авария на един от захранващите блокове, системата продължава своята работа като алармира системния администратор. Важна особеност на системите за отказоустойчивост е възможността за замяна без изключване на системата (hot spare). Така, авариралият захранващ блок може да бъде демонтиран и сменен с изправен без изключване електрозахранването на компютърната система.

В особено важни системи, например с космическо и военно предназначение се прави тройно дублиране на управляващите системи. Всяка управляваща система получава информация от наличните датчици и взема решения за промяна на траекторията, промяна на работната среда и др. При тройно-дублираните системи се приема за вярно това решение, което се взема от две от трите управляващи системи, когато другата система е повредена.

Съвременните операционни системи поддържат функция за горещо поправяне (hot fixing) на повредени дискови данни. При откриване на грешен сектор от диска, драйверът на отказоустойчивостта се опитва да премести данните в добър сектор и да отбележи повредения като лош – забранен за използване. Защо е възможно това? Ако секторът е физически повреден,

той не може да се прочете, данните се губят и не е възможно да се възстановят. На практика дисковете се повреждат постепенно. Части от покритието на диска с по-лошо качество губят възможностите си за четене-запис. При това прочитането е възможно след няколко поредни опита. Входно-изходният драйвер проверява колко опита за четене са направени, ако е премината зададената граница, определя сектора като повреден и премества успешно прочетения сектор. Възможно е драйверът да извършва контролно четене на записаната информация, за да установи повреда на сектора. Това е известно като Read-After-Write и се използва при оптическите системи за съхраняване на информация. При твърдите дискове не се използва, тъй като ще доведе до голямо натоварване на дисковата система и забавяне на нейната работа.

Най-често се използват системи за отказоустойчивост на данните реализирани чрез RAID технология за защита на данните, съхранявани на твърди дискове. За да има устойчивост, системата трябва да е преосигурена, да има излишък, дублиране на информацията (redundancy). Създават се надеждни масиви от нескъпи дискове RAID (Redundant Array of Independent/Inexpensive Disks). Съществуват различни нива на RAID, с различни възможности.

RAID 0 – Лентов набор (Disk Stripping)

Съдържанието на дисковете се разглежда като блокове (клъстери) с размер 64KB. Данните се разполагат последователно във всички дискове от масива. Тъй като няма излишък на данните, няма никаква отказоустойчивост. Обратно, вероятността за дефект на системата се увеличава, при отказ на един от дисковете в масива се губи цялата информация. Тогава защо се използват лентовите набори:

1) Те позволяват създаване на голям обем дисков масив чрез обединяване на множество дискове (за Windows сървърите до 32).

2) Увеличава се бързодействието на дисковата система в сравнение с бързодействието на всеки от твърдите дискове. Например, за система от два диска с лентов набор, времето за четене и запис е два пъти по-малко от това на отделния твърд диск, тъй като дисковете операции се разпределят по двете независими устройства.

RAID 1 – Огледални дискове (Disk Mirroring)

За дублиране са необходими два твърди диска, препоръчително е те да са с еднаква големина (еднакъв брой LBA[1] блокове). Вторият диск съдържа точно (огледално) копие на първия диск. Първият диск е основен (primary), вторият е архивен (secondary). Ако един от дисковете се повреди системата продължава работа без прекъсване. RAID 1 се реализират чрез интегриран на дънната платка или външен (PCI, PCI-X) RAID контролер. Препоръчва се използване на дуплексиране – всеки твърд диск работи със собствен дисков контролер. Ако двата диска използват общ дисков контролер, то неговото авариране спира цялата система, въпреки дублирането на информацията. Най-често се използват два еднакви SATA твърди диска. „Гореща” замяна в този случай не е възможна.

При RAID 1 времето за четене е два пъти по-малко отколкото на твърдия диск, времето за запис е същото. При използване на големи области от последователни блокове от данни (големи файлове), четните блокове се намират на първия диск, нечетните – на втория. При четене половината информация се прочита от диск 1, другата половина от диск 2 – съответно времето за четене е два пъти по-малко. При запис информацията се записва едновременно на двата твърди диска, времето за запис е без промяна.

RAID 3 – Лентов набор с големи блокове (Disk Stripping with Large Blocks)

Използват се големи блокове данни. Използва се отделен диск за проверка на данните. RAID 3 включва три твърди диска. Подобно на RAID 0 информацията се разделя на блокове,

[1] LBA (Logical block addressing,) е начин на адресиране на големите твърди дискове. Нормално твърдите дискове бяха проектирани да се адресират по тяхната физическа структура – (CHS, Cylinder-Head-Sector) – номер на цилиндър (пътечка, номер на записваща глава, номер на сектор). Ограничението на CHS системата е до 1024 цилиндъра, 16 глави и 63 сектора. Съвременните твърди дискове надхвърлят тези ограничения. Методът на адресиране LBA разделя диска на области от 512 или 1024 байта (за компакт дисковете, стандарта ISO 9660 определя размер на блока 2048 байта).

които се записват последователно на първия и втория диск. В третия диск се записва блок данни, като всеки байт е изчислен като ИЗКЛЮЧВАЩО ИЛИ на данните от първия и втория диск.

ИЗКЛЮЧВАЩО ИЛИ (XOR) е битова операция със следната функция:

A	B	C=A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Характерно за ИЗКЛЮЧВАЩО ИЛИ е обратимостта:

C = A XOR B
B = A XOR C
A = B XOR C

На първия диск записваме стойности A, на втория – B, на третия – контролен – C.

Ако диск A се повреди, неговите данни се определят като „B XOR C". Ако се повреди диск B, съответно - "A XOR C. Ако се повреди диск C не е необходимо да се прави изчисление, той не съдържа данни. Ако се повредят два от дисковете информацията се губи.

Времената за четене и запис са както при RAID 1.

RAID 5 – Лентов масив с контрол по четност (Stripping with Parity)

Това е най-популярният RAID метод. Поддържат се минимум 3, максимум 32 твърди диска. За разлика от RAID 3 няма отделен диск за корекция на грешки, коригиращата информацията се разпределя и записва на всеки от дисковете в масива. При повреда на едно устройство, на останалите има достатъчно служебна (коригираща) информация за възстановяване на съдържанието на повреденото устройство. Повреда на два диска води до загуба на данните в масива.

RAID 5 обикновено се реализира с блок от дискове проектирани за замяна без изключване (hot spare). Вижте снимката на SAN, всеки диск има индикатор за нормална работа, индикатор за грешка, дръжка за изваждане.

RAID 10 – Огледални дискови масиви (Mirrored Disk Arrays)

RAID 10 създава два идентични RAID 0 дискови масива. За всеки твърд диск от първия масив се създава огледален образ върху друг твърд диск от другия масив.

Виж още: Клъстериране

Въпроси

1. Какви са предимствата на Smart UPS пред Back UPS?
2. Защо цената на Smart UPS е по-висока от Back UPS със същите характеристики?
3. Коя система RAID 0 или RAID 1 предлага по-добра отказоустойчивост?
4. Каква е ползата от системата за горещо поправяне (hot fixing)?
5. Какво представлява възможността за замяна 'hot spare'?
6. Какви дейности включва политиката за архивиране?