DNMI DET NORSKE METEOROLOGISKE INSTITUTT

klima

DATABASEPROSJEKTET I KLIMAAVDELINGEN
SIKKERHETSRUTINER
Delprosjekt 7.8.

TOM AASEN

RAPPORT NR. 08/93 KLIMA

DNMI-RAPPORT

DET NORSKE METEOROLOGISKE INSTITUTT
POSTBOKS 43 BLINDERN 0313 OSLO 3

TELEFON: 22 96 30 00

ISBN

RAPPORT NR.
8/93 KLIMA

DATO
2.3.93

TITTEL

DATABASEPROSJEKTET I KLIMAAVDELINGEN,
SIKKERHETSRUTINER.
Delprosjekt 7.8.

UTARBEIDET AV

Tom Aasen.

OPPDRAGSGIVER

DNMI-Klimaavdelingen

SAMMENDRAG

Datasikkerheten må ivaretas også i prosjektperioden til databaseprosjektet. Det viktigste i denne omgangen er å forhindre tap av programmer, strukturer, applikasjoner og lignende. Dette gjøres best ved sikkerhetskopiering. De vanligste metodene er beskrevne og vurderte. Det er gitt tilrådninger om hva som kan være å foretrekke av metodene.

UNDERSKRIFT

Tom Aasen
Tom Aasen
PROSJEKTLEDER

Bjørn Aune
Bjørn Aune
FAGSJEF

INNHOLDSFORTEGNELSE.

1. Definisjoner.

DBA er database administrator.

Databasefiler er de filene som inneholder de dataene som er i tabellene.

Redo Log filer er filer som inneholder transaksjoner/endringer som er gjort på databasen. Redo Log filene og sikkerhetskopien er viktige ved gjenoppretting av databasen etter et havari av datasystemet. Minimum antall av disse filene er to stykker. De må ha en minimumsstørrelse og dette kan slåes opp i Database Administrators Guide [1]. Redo Log filene går på rundgang. Når den siste er full begynner databasesystemet å overskrive den første hvis annet ikke er satt.

Checkpoint er markeringer mellom hver gang databasesystemet skriver alle databaseblokkene som har blitt modifiserte, både de blokkene som det er utført Commit på og de som dette ikke er utført på, ned på databasefilene. Intervallet mellom hvert Checkpoint er satt av DBA. I tillegg setter databasesystemet nytt Checkpoint hver gang Redo Log filene skifter.

Log Switch er betegnelsen på vekslingen mellom to Redo Log filer.

Rådata er ubehandlede data fra observasjonsstasjonene.

Control filer er filer som inneholder opplysninger om databasen som for eksempel navnene på Redo Log filene, navnet på databasen og når databasen ble opprettet. Minst en slik fil må eksistere for at databasen skal ha noen funksjon. Oracle kan håndtere mange Control filer samtidig. Control filene **skal** legges på fysisk forskjellige steder i datamaskinsystemet. Dette er for å redusere sannsynligheten for at informasjonen fra disse filene kan gå tapt.

Datatap er tap av data (filer, filsystemer etc.) som ligger på disk.

2. Innledning.

Dette prosjektet skal se på sikkerheten med hensyn til datatap ved eventuelle uhell i prosjektfasen. Dette kan løses ved sikkerhetskopiering av databasen og arbeidsområdene til prosjektdeltagerene. EDB-avdelingen har sørget for at dette er blitt utført på Klimaavdelingen sitt Nord-datasystem til i dag. Dette prosjektet skal sørge for at noe tilsvarende blir gjort på det nye datasystemet under prosjektfasen. Siden vi ikke har så stor erfaring med databaser, ble det i denne omgangen ikke sett på rettighetene til utviklerne. Dette er noe som kanskje bør sees på i den overnevnte perioden, men dette får bli opp til Database-gruppen og DBA å vurdere etterhvert som prosjektet skrider fram.

3. Hvorfor sikkerhetskopiering.

Ved feil i datasystemer er det ønskelig å ikke få datatap eller i hvertfall få redusert datatapet til et minimum. Ut fra en vurdering av de lagringsmediene en har i dag, bør det gjøres visse tiltak. I dag skiftes ikke lagringsmedier før de går i stykker. Dette kan medføre vanskeligheter med å få gjenvunnet dataene. I verste fall er alle dataene tapt. Menneskelig feil er heller ikke til å unngå. Det er fort gjort å slette for mye. Disse to eksemplene (blant flere) viser at hvis data kun ligger på et sted og det ikke finnes kopier av dem, er datasystemet sårbart for datatap. Derfor er det viktig at det finnes en god sikkerhetskopierings-rutine.

4. Rutine.

4.1 Innledende studier.

Dette prosjektet har gått en stund. Allerede våren 1992 ble det tatt kontakt med EDB-avdelingen for å se på sikkerhetskopiering av klimadatabasen. På det tidspunktet var det ikke gjort mye. Det var kun tatt en kopi og denne var flere måneder gammel. Det ble på dette tidspunkt presisert at vi så på sikkerhetskopiering som særdeles viktig.

4.2 Sikkerhetskopisystem.

Senere er det blitt gjort en del. EDB-avdelingen har kjøpt inn et sikkerhetskopi-system. Det heter Networker System. Dette systemet er plasskrevende og tar mye ressurser, men det er et fullblods sikkerhetskopi-system. Det har en database som tar vare på informasjonen fra systemet ved kopiering (hvilke filer som ligger hvor, når de ble kopierte og så videre). En kan bestemme ned til enkeltfiler over hva som skal kopieres og når. Det hele er pakket inn i et grafisk grensesnitt som virker meget oversiktlig. Det vil bli mulig for andre enn de som tar sikkerhetskopiene, til å bruke dette systemet for å følge med hva som skjer. Eventuell uthenting av filer og kataloger fra systemet skulle ikke by på problemer med dette hjelpemiddelet. Kopiene blir lagt på 8mm kassettmagnetbånd der hver av dem rommer opptil 2GB. Båndstasjonen er montert i Typhoon.

Sikkerhetskopiene blir for tiden lagt ned på mange bånd (antallet er noe diffust, men det er mange nok). Båndene ligger i pengeskapet ved printerene i 4. etasje.

4.3 Hvordan sikkerhetskopieringen forgår.

Det overnevnte sikkerhetskopi-systemet er nokså nytt og uprøvet her. Derfor hadde Geir Austad i begynnelsen kontroll med denne kopieringen. Nå har EDB-operatørene overtatt denne oppgaven. For tiden utføres det hver uke to sikkerhetskopieringer på de områdene på Typhoon som er av interesse for oss. Natt til fredag taes det en full kopiering. Natt til tirsdag taes det en redusert en. De kataloger som kopieres og som er av interesse for oss, er følgende:

/usr4 og alle under denne, (inkluderer alle brukerne på KA).

/usr/people og alle under denne.

/klima/files og alle under denne,(inkluderer klimadatabasen).

En del filer blir ikke kopiert. Det er alle "core-" og "objekt"-filer. Natt til onsdag kopieres bare de filene som er forandret (inkrementell sikkerhetskopiering).

4.4 Innsetting av sikkerhetskopi.

Foreløpig er dette systemet såpass nytt for oss alle at det er vanskelig på dette tidspunkt å legge opp en fastspikret rutine for å få databasen operativ etter et avbrudd. Derfor må det utføres tester som danner grunnlaget for denne rutinen. Dette er ikke blitt gjort enda, men EDB-avdelingen er blitt henstilt om å se på dette. Dette haster fordi det er mistanke om at den sikkerhetskopien som taes i dag, ikke er tilstrekkelig og derfor ikke kan brukes til å bygge opp databasen på nytt hvis hele eller deler av den skulle gå tapt. Det bør snarest utpekes en fra databasegruppen som følger opp denne saken.

Hvem som eventuelt får jobben med å legge tilbake dataene i Klimadatabasen etter eventuelle avbrudd, må vurderes. EDB-operatørene vil kunne klare å legge sikkerhetskopier tilbake på maskinen, men når databasen skal taes opp igjen krever det kunnskaper som operatørene ikke har (i dag). DBA bør ha denne oppgaven inntil videre. Senere kan dette eventuelt delegeres, men DBA vil i alle tilfeller være en nøkkelperson og bør ha hovedansvaret.

5. Anbefalinger.

5.1 Sikkerhetskopi-metoder.

Det er flere måter å utføre sikkerhetskopiering på Oracle databaser. Metodene har sine fordeler og ulemper. I Oracle sin Database Administrators Guide [1] står dette mer inngående beskrevet. Under er hovedtrekkene i de to vanligste måtene å sikkerhetskopiere en Oracle database beskrevet.

5.1.1 Når databasen stoppes.

Databaseansvarlig (eller en med slike rettigheter) må ta ned databasen. Etterpå kan en bruke vanlige kopieringskommandoer eller et kopieringssystem. Alle databasefilene, Redo Log filene og en av Control-filene kopieres til et dertil egnet sted.

5.1.2 Når databasen går.

Databasen må gå med ARCHIVELOG på til daglig.

SQL-kommando:
-**ALTER TABLESPACE** tabellområde-navn **BEGIN BACKUP**

Kopier (bruk gjerne et sikkerhetskopi-system) databasefilene, en Controlfil og eventuelt offline Redo Log filene til et dertil egnet sted. Få også med de Redo Log filene som har blitt skrevet til mens sikkerhetskopieringen har foregått.

SQL-kommando:
-**ALTER TABLESPACE** tabellområde-navn **END BACKUP**

Det er meget viktig at ALTER-kommandoene er utført. Hvis ikke blir kopien ufullstendig.

5.2 Vurdering av metoder.

For å bestemme hvilken sikkerhetskopieringsmetode en skal bruke må en vurdere spesielt to forhold. Det er hastigheten på databasesystemet, driftsstans en gang i døgnet og eventuelt tap av data. Dertil kommer ressurser for administrasjon av sikkerhetskopieringen og tilbakelegging av sikkerhetskopierte data.

5.2.1 Databasen stoppet.

Hvis man kan tolerere at databasen ikke er tilgjengelig i en periode en gang i døgnet, kan man kjøre databasen i NOARCHIVELOG-mode. Redo Log filene kan da komme til å rullere. Det betyr at hvis det ikke er flere ledige Redo Log filer som databasen kan bruke, vil databasesystemet ta den eldste Redo Log fila og skrive over denne. Dette betyr at en bør ha tilstrekkelig mange Redo Log filer slik at overskriving ikke finner sted. Hvis noen eller alle Redo Log filene blir overskrevet før neste sikkerhetskopiering, kan en ikke gjenopprette databasen opp til siste checkpoint.

5.2.2 Databasen går.

For å ta sikkerhetskopi mens databasen er oppe må ARCHIVELOG'en være på. Dette gjør at Redo Log filene blir kopiert til et område bestemt av DBA. Derfra kan Redo Log filene kopieres til et annet mer egnet område (for eksempel magnetbånd) sammen med de andre databasefilene og Controlfila. Alle transaksjoner opp til start av sikkerhetskopieringen vil komme med i denne operasjonen.

Det er forslag fra EDB-avdelingen om å la Oracle lagre Redo Log filene direkte på magnetbånd. Om dette er mulig på Silicon Graphics plattformer må sjekkes med Oracle. Uansett krever det en del lagringsplass og hvis bruk av magnetbånd, krever denne metoden at noen skifter båndene når de går fulle.

Antageligvis vil hastigheten på databasesystemet gå ned med denne metoden. Hvor mye må undersøkes.

5.2.3 Ved EXPORT.

Det er også mulig å bruke programmet, EXPORT, for å ta kopi. Den bør brukes når en skal transportere data mellom databaser (med for eksempel forskjellige versjoner), mellom maskiner eller for å arkivere data. EXPORT er ressurs- og tidskrevende, men det er mulig å ta inkrementell EXPORT (bare tabeller som er endret). Dette kan redusere belastningen en god del både for maskin og i tid. Det bør være liten aktivitet på databasen ved EXPORT. Fordelen med å ha data lagret med denne metoden er at de kan hentes inn igjen i en annen database. Det betyr at hvis originaldatabasen ikke kan gjenopprettes i den form den hadde (for eksempel at control-filene er blitt borte), kan man likevel opprette en database med de samme dataene forholdsvist enkelt og raskt.

5.3 Når utføres sikkerhetskopiering.

I utviklingsfasen kan vi tolerere at databasen tas ned i kortere perioder. Derfor kan sikkerhetskopieringsrutinene som i dag går, få fortsette med det, men når databasen går operasjonelt er det stor sannsynlighet for at vi ikke kan tolerere avbrekk. Det betyr at vi høyst sannsynlig vil la databasen gå med ARCHIVELOG'en på i fremtiden og ta full sikkerhetskopi av databasen en gang i døgnet som også er det vanlige.

Med ARCHIVELOG'en på kan delvis sikkerhetskopiering foregå når som helst på døgnet, men full sikkerhetskopiering bør legges til tider med liten belastning av datasystemet (natten fortrinnsvis).

5.4 Lagring av sikkerhetskopier.

Vi bør ha flere sikkerhetskopier liggende. Et passende antall fulle sikkerhetskopier er fem stykker. Det kan med fordel være mer enn en kopi fra forrige døgn. En av disse kopiene lagres i et pengeskap eller tilsvarende.

Det anbefales likevel på det sterkeste å ta vare på noen eldre kopier i tillegg (inntil et år gamle). Minst en av disse kopiene som helst er laget ved hjelp av EXPORT-kommandoen, lagres på et helt annet sted enn Blindern. Alle kopier skal oppbevares utilgjengelig for alle andre enn de få som har den nødvendige klareringen.

Det bør vurderes om kopiene bør krypteres. Det er lett å få med seg hele Klimadatalageret hvis det er lagt ned på de nye typene magnetbånd. (En liten kassett som med letthet kan puttes i bukselommen, rommer opptil 2GB og det er omtrent 1/4 av hele klimalageret.)

Hvis rådata blir lagret holder det med sjeldnere sikkerhetskopiering. Hyppigheten kan vurderes senere. Det bør være minst to kopier hvorav en er lagret på et annet sted enn Blindern. Kryptering må også her vurderes.

DBA bør ha hovedansvaret for sikkerhetskopieringen. Dokumentasjon og lagring av sikkerhetskopier skal utføres i henhold til kvalitetssikrings-håndbok for databasen.

5.5 Kommandoer for gjenoppretting av databasen etter avbrudd.

RECOVER kommandoen brukes for å hente inn sikkerhetskopien av databasen. Den er beskrevet i Oracle sin Database Administrators Guide [1]. En kan hente tilbake enkelttabeller, tabellområder eller hele databasen. Det er også mulig å kopiere tilbake databasen opp til et valgt tidspunkt. For å kopiere hele databasen må den være tatt ned. I de andre tilfellene kan den være oppe.
Hvis en skal hente inn data som er lagt ut ved EXPORT-kommandoen, må en bruke IMPORT-kommandoen.

6. Egne sikkerhetskopier.

Det er fullt mulig å selv legge data på magnetbånd. I dag har vi to muligheter, enten på magnetbåndstasjon eller på DAT. Magnetbåndstasjonen Kennedy og bruk av denne er beskrevet i rapport fra delprosjekt "Data inn" [2] (denne rapporten er under utarbeidelse i skrivende stund).

6.1 Maskinvare.

Av DAT-båndstasjoner finnes det flere, men den som er av mest interesse for oss, er den som befinner seg i arbeidsstasjonen Gust. Betjeningen av denne foregår fra en hvilken som helst arbeidsplass med tilknytning til Ethernettet og Unix. Det eneste en må utføre fysisk på magnetbåndstasjonen, er å sette inn båndkassetten og fjerne den når en er ferdig. Selve båndet rekvireres fra EDB-avdelingen via en av teknikerne (60M bånd rommer i overkant av 1 GB).

Betjeningen av DAT-stasjonen foregår ved hjelp av forskjellige programvarer. Brukes en arbeidsstasjon med grafisk grensesnitt mot Unix, finnes det grafiske programvarer. Ellers er det greit nok å bruke Unix (eller eventuelt programvarehuset FTP) sine programmer.

6.2 Kommandoer

Under Unix bør en kjenne til kommandoene tar og mt. Bruk man-kommandoen i Unix for mer inngående opplysninger om disse. Under kommer noen eksempler på bruk av disse kommandoene. Kommandoene under gjelder for den lokalt oppsatte båndstasjonen.

tar cv tekst.asc
Legger fila tekst.asc inn på båndet. Det er mulig å bruke stjerne (*) i filnavnet for å få med seg flere filer i en kommando.

mt fsf 1

Flytter pekeren (spoler) til tar-fil nummer 1 på båndet. Pekeren må flyttes ellers vil tar-fil 0 bli overskrevet ved ny tar cv ... kommando. (Tar-fil nummer 0 er den første på båndet. Hver tar-fil inneholder flere masselagerfiler (dos-filer, unix-filer etc).)

mt rew
Flytter pekeren til begynnelsen av båndet.

tar tv
Viser hva som ligger på den tar-fila pekeren peker på.

tar xv
Henter ut data fra båndet.

mt feom
Flytter pekeren til etter siste tar-fil på båndet.

Det kan være noe diffust å holde rede på hva som ligger på båndene og hvor. Dette krever at en fører protokoll når en legger filer ned på båndene.

Det er/vil bli lagt inn verktøy fra programvarehuset FTP [3] som kan utføre tilsvarende fra PC. Programmene vil ligge under katalogen PCTCP. Det vil bli laget en egen rapport for bruk av disse verktøyene senere.

Referanseliste

[1] Oracle RDBMS, Database Administrators Guide versjon 6.0.

[2] Rapport fra delprosjekt 7.1, Data inn (som er under utarbeiding).

[3] PC/TCP Network Software manual, versjon 2.1. FTP Software, Inc.