STATENS IT

Backuppolitik i Statens It's standarddriftsplatform

Aftalekompleksets bilag 11 – Statens It's standarddriftsplatform
Underbilag B version 2017-1
Version 2017-1

10. januar 2017

STATENS IT

Indhold

1 Indledning

10. januar 2017
Version 2017.1

Statens It tilbyder, som en del af standarddriftsplatformen, at tage backup af løsninger. Der kan være forskellige årsager til at tage backup af en løsning, men hovedårsagen er at kunne genskabe ud fra en backup.

Dette dokument er et underbilag til bilag 11 i aftalekomplekset og har til formål, at beskrive forskellige backupscenarier med henblik på at kunne vælge den rigtige til en given løsning samt beskrive hvilken backup der leveres som standard.

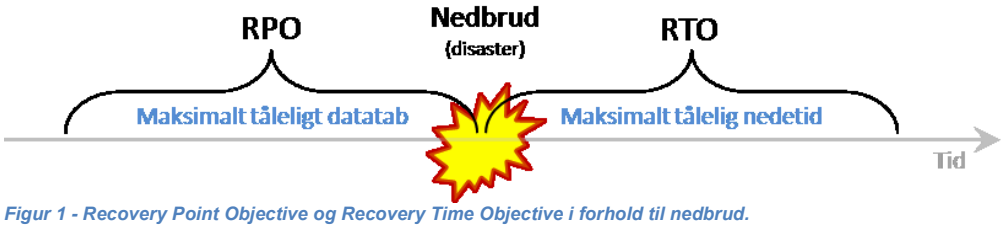
1.1 Afgrænsning

Statens It tager også backup af AS-IS miljøerne, altså de driftsmiljøer der er etableret før Statens It. Denne backup udføres i tråd med nærværende dokuments beskrivelser, men ligger uden for dette dokuments rammer, at gå i dybden med. Det er blot vigtigt at holde sig for øje, at det er de samme kriterier der bør ligge til grund for backup af AS-IS miljøet.

2 Terminologi

Backup handler om at kunne genskabe en løsning, som den så ud på et givent tidspunkt. Med givent tidspunkt menes et tidspunkt tilbage i tiden, hvor der er lavet et øjebliksbillede af løsningen i form af en backup. Ordet løsning dækker over et system, systemkonfiguration og data, alt afhængig af løsningens komponenter.

Behovet for backup er knyttet til de forretningsmæssige krav, der stilles til en given løsning. Disse forretningsmæssige krav kan udtrykkes ved brug af fagtermer inden for backup og forklares nedenfor.



Figur 1 - Recovery Point Objective og Recovery Time Objective i forhold til nedbrud.

2.1 Nedbrud

Nedbrud dækker over det engelske begreb ”disaster” som bedst oversættes til ”katastrofe”. Vi har valgt at bruge ordet nedbrud, da det i denne sammenhæng bedst beskriver den egentlige hændelse.

I dette dokument beskrives et nedbrud som den tilstand af en løsning, der gør at løsningen kun kan bringes i drift ved indlæsning af en backup. Det er altså ikke blot et driftsstop, men et tab af mindst en komponent, der gør at man ikke blot kan genstarte serveren og bringe løsningen i drift igen. En komponent kan f.eks. være en harddisk på en fysisk server eller en hel virtuel server, der slettes som følge af en software fejl.

Et nedbrud af denne type vil være forbundet med nede tid på løsningen og muligt datatab. Forretningsområdet vil ikke være it-understøttet i den tid det tager at genetablere løsningen ud fra backup.

Tidspunktet for nedbruddet vil være udgangspunktet for de følgende begreber, som drejer sig om mål (objective).

2.2 Recovery Point (RP)

Recovery Point er et tidspunkt, hvor der etableres et øjebliksbillede (en backup) af løsningen, som man kan komme tilbage til, altså genskabe løsningen ud fra.

2.3 Recovery Point Objective (RPO)

Recovery Point Objective dækker over det maksimale tidsrum, hvor forretningen kan tåle datatab, som følge af et nedbrud. Se *Figur 1*.

2.4 Recovery Time (RT)

Recovery Time er den tid det tager at genskabe en løsning ud fra et øjebliksbillede (en backup) fra et givent *Recovery Point*.

2.5 Recovery Time Objective (RTO)

Recovery Time Objective dækker over det maksimale tidsrum forretningen kan tåle at løsningen er ude af drift, som følge af et nedbrud. Se *Figur 1*.

3 Backupscenarier

Det er vigtigt, at forretningen for hver enkelt løsning forholder sig til backup og afgør, hvad det forretningsmæssige behov er. De forretningsmæssige behov for backup falder typisk i nedenstående tre scenarier. Det er vigtigt at forholde sig til alle scenarier, da der kan være behov for at dække mere end et af scenarierne.

3.1 Disaster recovery

Et *disaster recovery* backupscenarie har til formål at kunne genskabe en løsning på baggrund af et nedbrud (*disaster*). Forretningen skal i dette scenarie forholde sig til RPO og RTO.

Eksempel:
Forretningen har for deres tilskudsløsning identificeret, at de maksimalt kan tåle tab af data svarende til en arbejdsdag. Altså en RPO på 24 timer. De har ligeledes identificeret at de maksimalt kan tåle at have løsningen ude af drift i 3 arbejdsdage, altså en RTO på 72 timer.

Backupløsningen skal etablere RP en gang i døgnet for at imødekomme RPO.

Statens It er driftsansvarlig og sikrer at den nødvendige backup etableres for at kunne genskabe løsningerne i forbindelse med denne form for nedbrud jf. afsnit 4. Det er dog en tillægsydelse til serverprisen, som kan fravælges.

3.2 Revisionshistorik

Et revisionshistorik backupscenarie har til formål at kunne genskabe en løsning på baggrund af en revisionsanmodning. Forretningen vil i mange tilfælde være underlagt krav om revision enten som følge af lovgivning eller som internt krav.

Eksempel:
En tilskudsløsning er underlagt krav om revision som følge af lovgivning. Lovgivning kræver at løsningen kan genskabes som den så ud fem år tilbage i tid. Kravene er formuleret således, at det kun er grundlaget for den årlige revision, der skal kunne genetableres.

Backupløsning skal etablere RP en gang årligt, som gemmes i fem år.

Statens It etablerer ikke som standard denne form for arkivering, da det udelukkende er et forretningsmæssigt behov, som er løsningsspecifikt. Ret henvendelse til Statens It såfremt der et behov for denne løsning.

3.3 Sikkerhedskopi

Et sikkerhedskopi backupscenarie har til formål at kunne genskabe en løsning på baggrund af en utilsigtet ændring. I dette tilfælde vil det ofte være data forbundet med en løsning og ikke selve løsningen, medmindre data og løsning er så tæt forbundet at det ikke giver mening af tage backup af det ene og ikke det andet.

Eksempel:
Den årlige prognoseberegning for tilskudsløsningen er gennemført succesfuldt. Tidligere har forretningen oplevet at prognosemodellerne ikke var intakte ved opstart af beregningsperioden, da andre modeller havde været afprøvet i løbet af året og havde efterladt løsningen i en ukendt tilstand.

For at sikre beregningsmodellerne imod utilsigtede ændringer i løbet af året, ønskes derfor en sikkerhedskopi oprettet, så denne kan genskabes til prognoseberegningerne det følgende år.

Backupløsningen skal etablere RP umiddelbart efter gennemført prognoseberegning, som gemmes indtil følgende års prognoseberegning er gennemført succesfuldt.

Statens It etablerer ikke som standard denne form for arkivering, da det udelukkende er et forretningsmæssigt behov, som er løsnings specifikt. Ret henvendelse til Statens It såfremt der et behov for denne løsning.

4 Standardbackup og recovery

Statens It leverer en standardbackup i henhold til et *disaster recovery* backupscenarie og i tilfælde af nedbrud genskabes løsninger til sidste succesfulde *recovery point.*

Backup gemmes for alle løsningskomponenter som standard i 60 dage med mindre andet er anført i nedenstående tabel.

Løsningskomponent	**Standardbackup (*recovery point*)**	**Kommentar**
Server	Daglig backup	Server benyttes her som en fælles betegnelse for: • Webserver • Applikationsserver • m.fl.
Database Oracle DBMS	Fuld backup 1 gang om ugen Incremental backup 1 gang i døgnet	Transaktionslog backup foretages som standard 1 gang i timen i dagtiden.
Database Microsoft SQL	Fuld backup 3 gange i dagtiden	
Database MySQL	Ingen	Håndteres efter aftale med Statens It
Database PostgrSQL	Ingen	Håndteres efter aftale med Statens It
Shared services	Daglig backup	Shared services benyttes her som en fælles betegnelse for: • Active Directory • Exchange (Mail/kalender) • Fil • Print • Webkontor • m.fl.

4.1 Recovery

Recovery time afhænger af sammensætningen og kompleksiteten i den konkrete løsning, herunder systemets beskaffenhed, dokumentation, antallet af komponenter i systemet og mængden af data.

4.2 Standard backup metode

4.2.1 Backup af virtuelle Servere

Der tages dagligt en backup af alle VMDK-filer ved brug af VMWare Snapshot, som gør SIT i stand til at restore både hele den virtuelle server eller enkelte filer og mapper på serveren.

Det er den type backup der anvendes som standard, hvor intet andet er ønsket, men kan dog vælges fra af kunden.

4.2.2 Filbackup med Netbackup agent.

Der tages backup af alle drev/filer på maskinen. På Windows platforme også System State.
Dette gør SIT i stand til at restore alle filer på serveren, men ikke selve serveren.
I en restore situation af hele serveren, er der brug for en tom server, som har de samme specifikationer som den oprindelige server, for at backuppen kan genskabes.
Fuld filbackup foretages en gang om ugen i weekenden.
Incremental filbackup foretages dagligt mandag til fredag.
Kan anvendes på fysiske og virtuelle servere.

4.2.3 MSSQL Backup

4.2.3.1 VMWare Snapshot backup med SQL

Der tages en backup af alle VMDK-filer på VMWare, samt en standard backup af alle databaser på SQL serveren. Hvilket sætter SIT i stand til at restore både den virtuelle maskine og/eller enkelte filer mapper på maskinen. SQL backup giver mulighed for at lave restore af alle de databaser som er på serveren.
Med denne metode kan der kun laves restore af databaserne til det tidspunkt hvor backup bliver taget (ingen point in time backup af databaserne).
Køres 3 gange dagligt i inden for normal arbejdstid, hele ugen.
Kan kun anvendes på virtuelle maskiner.

4.2.3.2 SQL backup med netbackup agent:

Der tages fuld backup af alle databaser samt transaktionslog af de databaser som er i fuld mode. Hvilket gør SIT i stand til at restore databaserne på en ny maskine. Med denne metode kan der laves restores af databaserne til et bestemt tidspunkt mellem to backupjob (point in time).
Der laves ingen backup af selve serveren, kun af databaserne serveren ved brug af denne metode.
SQL fuld backup køres dagligt.
Transaktionslog backup køres 3 gange dagligt i inden for normal arbejdstid, hele ugen.
Kan anvendes på fysiske og virtuelle maskiner.

4.2.4 ORACLE Backup

Der tages backup af ORACLE Databaser ved hjælp af RMAN, samt kald af scripts som ORACLE-Team har udviklet.
Der laves ingen backup af selve serveren, kun af databaserne serveren ved brug af denne metode.
Kan anvendes på fysiske og virtuelle maskiner.
Backup type og schedule aftales med SIT Oracle team.

5 Forretningsspecifik backup

I de tilfælde, hvor standardbackup ikke er fyldestgørende, er det vigtigt at forholde sig til og præcisere behovet for backup. Her kan scenarierne i afsnit 3 - Backupscenarier tages i brug. Statens It yder rådgivning i forbindelse med specificering af backup behov for løsninger.