



Backuppolitik i Statens It's standarddriftsplatform

Aftalekompleksets bilag 11 – Statens It's
standarddriftsplatform
Underbilag C
Version 2015-2

Indhold

1	Indledning	3
1.1	Afgrænsning	3
2	Terminologi	4
2.1	Nedbrud	4
2.2	Recovery Point (RP)	4
2.3	Recovery Point Objective (RPO)	4
2.4	Recovery Time (RT)	4
2.5	Recovery Time Objective (RTO)	4
3	Backupscenarier	5
3.1	Disaster recovery	5
3.2	Revisionshistorik	5
3.3	Sikkerhedskopi	5
4	Standardbackup	7
5	Forretningsspecifik backup	8

1 Indledning

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.

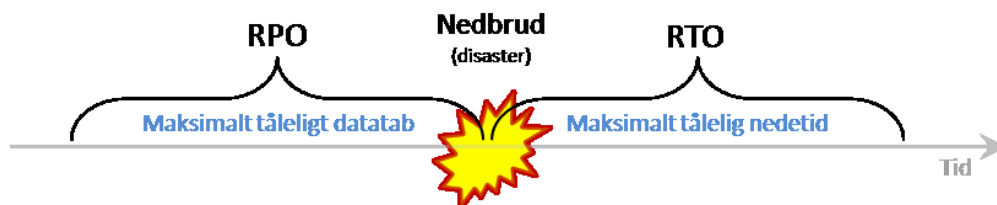
1.1 Afgrænsning

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 dokumentets beskrivelser, men ligger uden for dette dokumentets 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 og data kan lagres på billige medier, da RT vil være under RTO.

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.

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 backup, da det udelukkende er et forretningsmæssigt behov, som er løsningsspecifikt.

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 backup, da det udelukkende er et forretningsmæssigt behov, som er løsnings specifikt.

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 (<i>recovery point</i>)	Kommentar
Server	Daglig backup	Server benyttes her som en fælles betegnelse for: <ul style="list-style-type: none">• Webserver• Applikationsserver• m.fl.
Database	Backup hver 4. time	Ugentlig fuld backup samt log backup hver 4. time mellem kl. 07-19
Shared services	Daglig backup	Shared services benyttes her som en fælles betegnelse for: <ul style="list-style-type: none">• 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.

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.