

X Konferencja PLOUG
Kościelisko
Październik 2004

Poziomy rozwiązania „Disaster Recovery”

Jarosław Łagowski

IBM Polska
e-mail: j.lagowski@pl.ibm.com

Abstrakt

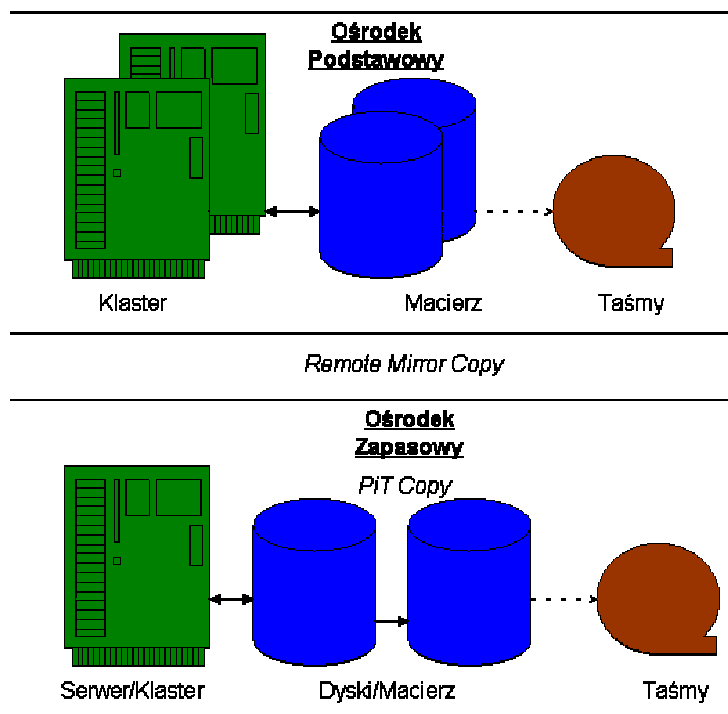
W roku 1992 organizacja użytkowników SHARE w porozumieniu z IBM zdefiniowała zestaw poziomów rozwiązania Disaster Recovery. Było to odpowiedzią na rosnące zainteresowanie rozwiązaniami DR i potrzebę ich klasyfikacji. Definicje ustalone przez SHARE okazały się bardzo pomocne dla realizacji projektów zabezpieczenia przetwarzania i dzięki swej elastyczności pozostają do dziś standardem klasyfikacyjnym. Referat obejmie prezentację podstawowych pojęć z zakresu "Disaster Recovery" oraz omówienie 7 (0-6) poziomów bezpieczeństwa DR wg klasyfikacji SHARE. Dodatkowy poziom 7, uwzględniony w referacie, dołączył do standardu SHARE w wyniku rozwoju technologii.

1. Definicje

1.1. Disaster Recovery

Disaster Recovery (odtworzenie po katastrofie) jest częścią *Business Continuity* – Zapewnienia Ciągłości. W ogólności, dotyczy to ciągłości działania danego przedsiębiorstwa lub instytucji. Żywną częścią przedsiębiorstwa lub instytucji jest oczywiście IT. Rozwiązania *Disaster Recovery* skupiają się na przywróceniu przetwarzania po awarii (katastrofie) uniemożliwiającej pracę w Ośrodku Podstawowym. Ośrodek Podstawowy rozumiany jest jako infrastruktura informatyczna (pomieszczenia, zasilanie, serwery, sieć, obsługa itp.) używana w czasie normalnej pracy przedsiębiorstwa lub instytucji.

Technologicznie, DR wspomagane jest przede wszystkim: lustrzanymi kopiami zdalnymi i błyskawicznymi kopiami lokalnymi PiT (*Point in Time*).



Rys. 1 Przykład architektury *Disaster Recovery*

1.2. Disaster Recovery Plan

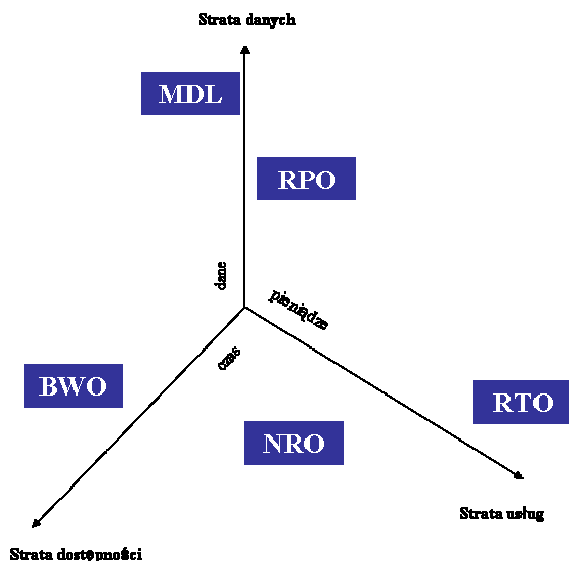
Disaster Recovery Plan (Plan Awaryjny) jest najważniejszym dokumentem w rozwiązaniu DR. Proces tworzenia tego dokumentu jest zasadniczym i nieustającym działaniem w ramach projektu DR. DR Plan opisuje całość rozwiązania i zawiera:

- analizę ryzyka i wymagań biznesowych,
- katalog procesów i aplikacji objętych projektem z określeniem ich parametrów DR (patrz 1.3),
- schemat organizacyjny dla projektu DR w rozróżnieniu na czas zwykłej pracy i czas katastrofy,
- schematy i procedury procesów DR (patrz 3.),

- scenariusze działania w przypadku katastrofy.

Plan Awaryjny jest dokumentem żywym i podlega cyklicznym rewizjom jak również zmianom będącym wynikiem ewolucji organizacyjno – technologicznej przedsiębiorstwa.

1.3. Parametry DR

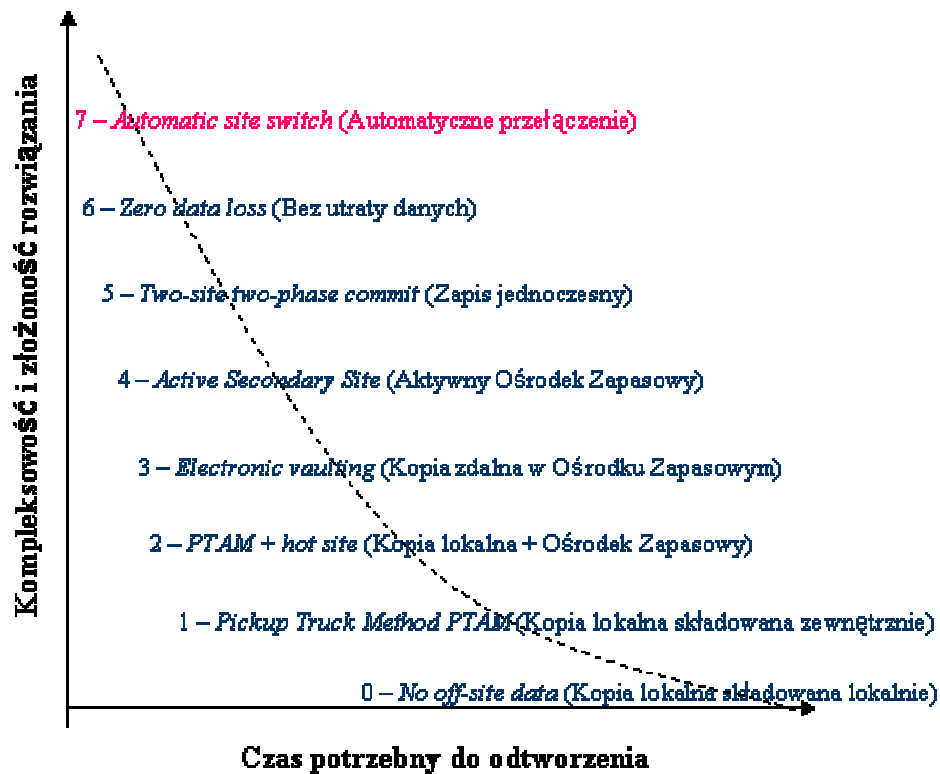


Rys. 2. Parametry DR

- **RTO – Recovery Time Objective**
Czas, który upływa od katastrofy do odtworzenia przetwarzania
- **RPO – Recovery Point Objective**
Aktualność danych odtworzonych po katastrofie, np. dane odtworzone z backupu wykonywanego co noc mają RPO równe –24 godziny
- **BWO – Backup Window Objective**
Zaburzenie dostępności systemu produkcyjnego, inaczej mówiąc, jak długa i jak częsta przerwa w przetwarzaniu (jeśli w ogóle) jest możliwa aby wykonać kopię DR
- **NRO – Network Recovery Objective**
Czas, który upływa od katastrofy do nawiązania awaryjnych połączeń sieciowych:
 - koniecznych do rozpoczęcia odtwarzania,
 - koniecznych do wznowienia przetwarzania,
 - docelowych po katastrofie.
- **MDL – Maximum Data Loss**
Maksymalna utrata danych z uwzględnieniem dodatkowych możliwości odtwarzania (logi transakcji, wprowadzenie dokumentów papierowych itp.).

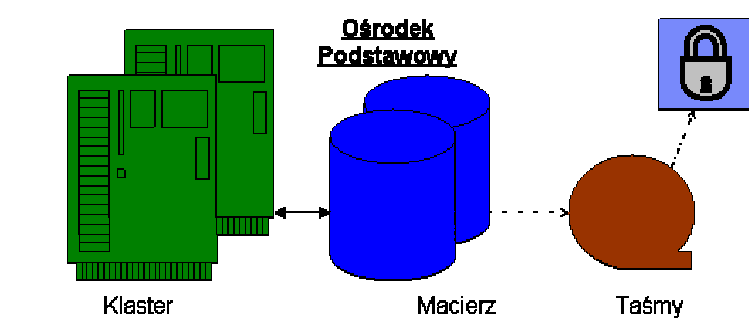
Podstawowymi parametrami, którymi operuje się w klasyfikacji poziomów DR wg SHARE są RTO i RPO.

2. Poziomy rozwiązania DR



Rys. 3. Poziomy rozwiązania DR

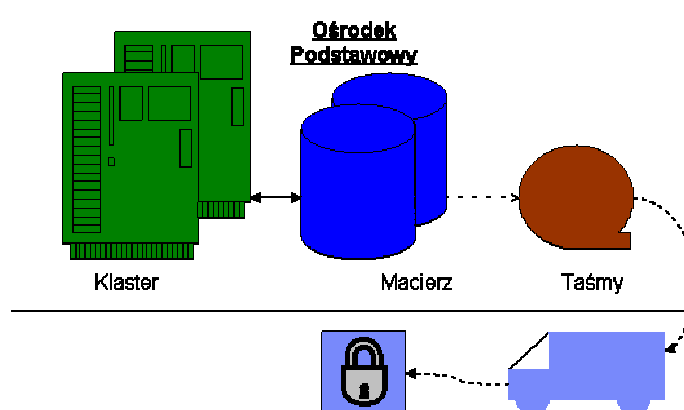
0 – No off-site data (Kopia lokalna składowana lokalnie)



Rys. 4. Poziom 0

- Wymagania *Disaster Recovery* nie są określone
- Brak Planu Awaryjnego, brak udokumentowanych procedur
- Dane są zabezpieczone kopią lokalną lub w ogóle
- Czas odtwarzania nie jest określony, być może odtwarzanie po katastrofie nie będzie możliwe
- RPO – częstotliwość kopii lokalnej – 24 godz.
- RTO – ?

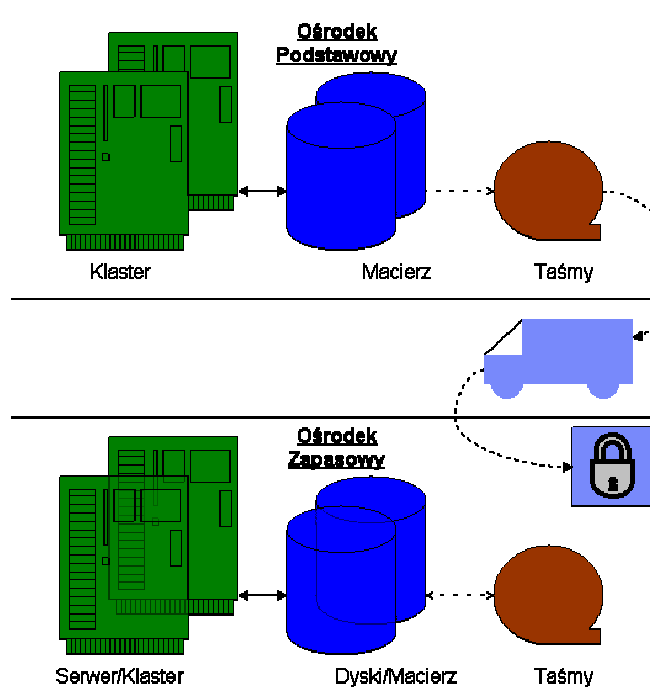
1 – Pickup Truck Method PTAM (Kopia lokalna składowana zewnętrznie)



Rys. 5 Poziom 1

- Niskie wymagania *Disaster Recovery*
- Plan Awaryjny jest zdefiniowany, istnieją udokumentowane procedury
- Dane są zabezpieczone kopią lokalną transportowaną fizycznie do oddalonego umiejscowienia
- Odtwarzanie zależy od tego jak szybko po katastrofie można odtworzyć infrastrukturę (przygotowane umiejscowienie, umowy z dostawcami).
- RPO – częstotliwość kopii lokalnej – 24 godz.
- RTO > 1 tydzień

2 – PTAM + hot site (Kopia lokalna + Ośrodek Zapasowy)

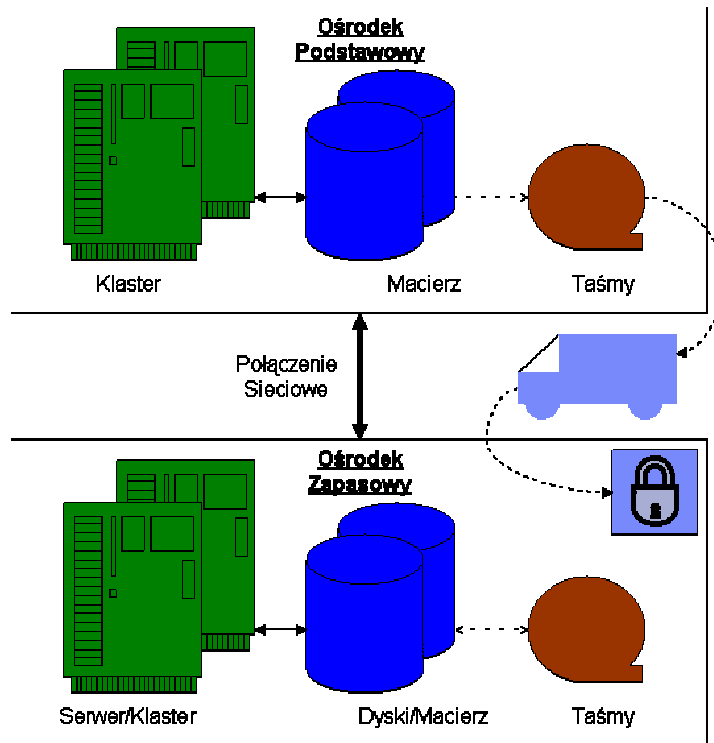


Rys. 6. Poziom 2

- Średnie wymagania *Disaster Recovery*

- Plan Awaryjny jest zdefiniowany, istnieją udokumentowane procedury
- Dane są zabezpieczone kopią lokalną transportowaną fizycznie do Ośrodka Zapasowego
- Odtwarzanie zależy od stopnia gotowości Ośrodka Zapasowego (przygotowana infrastruktura, umowy z dostawcami).
- Czas odtwarzania zwykle przekracza jeden dzień.
- RPO – częstotliwość kopii lokalnej – 24 godz.
- RTO > 1 dzień

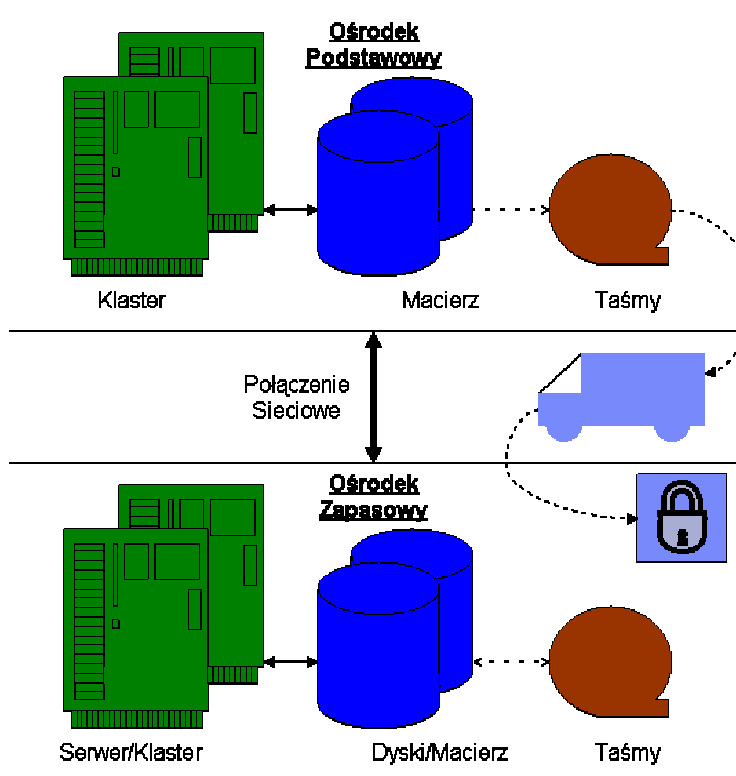
3 – Electronic vaulting (Kopia zdalna w Ośrodku Zapasowym)



Rys. 7. Poziom 3

- Podwyższone wymagania *Disaster Recovery*
- Plan Awaryjny jest zdefiniowany, istnieją udokumentowane procedury
- Dane są zabezpieczone kopią zdalną bezpośrednio w Ośrodku Zapasowym
- Odtwarzanie jest szybkie. Ośrodek Zapasowy musi mieć przynajmniej odpowiednią przestrzeń dyskową (do odbioru kopii zdalnej)
- Czas odtwarzania zwykle wynosi jeden dzień
- Musi istnieć połączenie sieciowe pomiędzy Ośrodkami zapewniające wykonanie kopii zdalnej.
- RPO – częstotliwość kopii zdalnej – 24 godz.
- RTO - 1 dzień

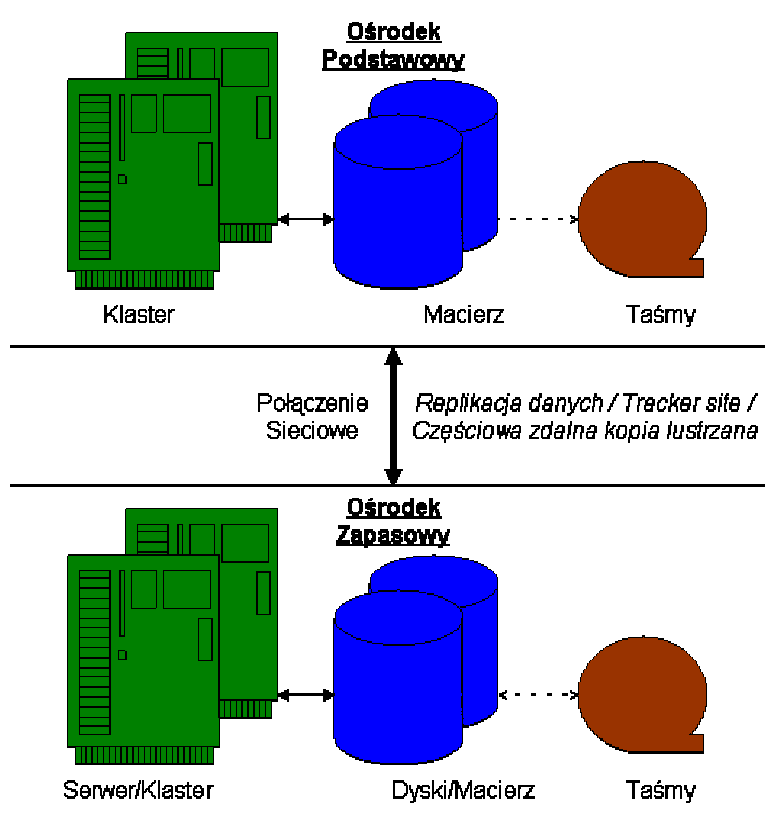
4 – Active Secondary Site (Aktywny Ośrodek Zapasowy)



Rys. 8. Poziom 4

- Wysokie wymagania *Disaster Recovery* .
- Plan Awaryjny jest zdefiniowany, istnieją udokumentowane procedury.
- Wybrane (lub wszystkie) dane są zabezpieczone kopią zdalną bezpośrednio w Ośrodku Zapasowym.
- Metoda PTAM może pozostać jako uzupełnienie.
- Odtwarzanie jest bardzo szybkie. Ośrodek Zapasowy może na bieżąco uczestniczyć w obciążeniu produkcyjnym. Wyposażenie i personel Ośrodka są kompletne.
- Czas odtwarzania zwykle wynosi poniżej jednego dnia.
- Musi istnieć połączenie sieciowe pomiędzy Ośrodkami zapewniające wykonanie kopii zdalnej
- Muszą istnieć połączenia sieciowe umożliwiające produkcję w Ośrodku Zapasowym
- RPO – częstotliwość kopii zdalnej – 24 godz.
- RTO < 1 dzień

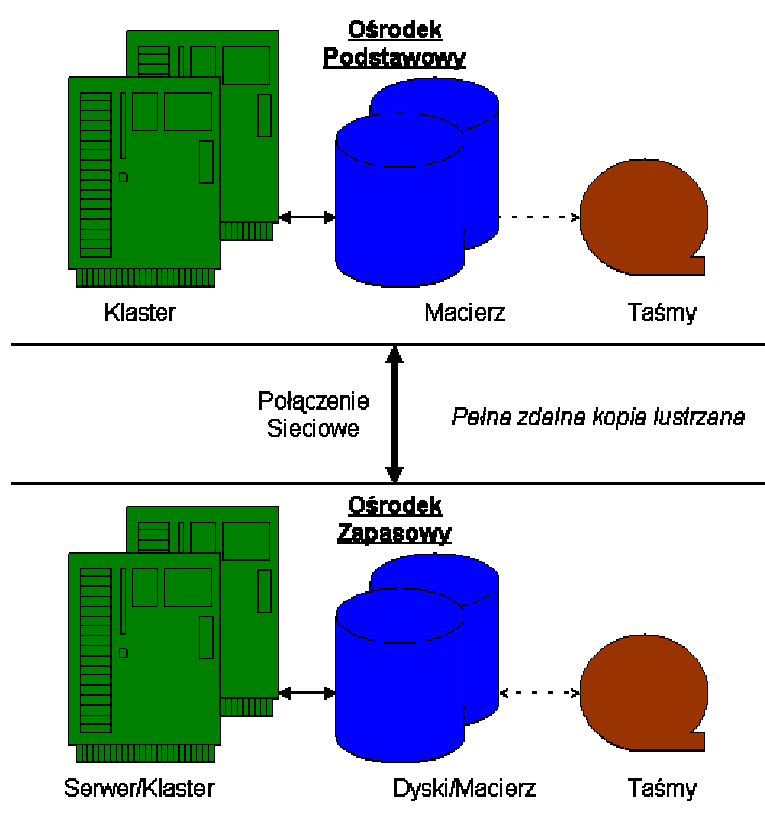
5 – Two-site two-phase commit (Zapis jednoczesny)



Rys. 9. Poziom 5

- Bardzo wysokie wymagania *Disaster Recovery*
- Plan Awaryjny jest zdefiniowany, istnieją udokumentowane procedury
- Dane, lub ich krytyczna część, są zabezpieczone poprzez mechanizm replikacji lub „two-phase commit” w Ośrodku Zapasowym
- Odtwarzanie jest bardzo szybkie. Dane lub ich krytyczna część są aktualne. Ośrodek Zapasowy może na bieżąco uczestniczyć w obciążeniu produkcyjnym. Wyposażenie i personel Ośrodka są kompletne.
- Czas odtwarzania zwykle wynosi poniżej 12 godzin.
- Musi istnieć połączenie sieciowe pomiędzy Ośrodkami zapewniające nieznaczące opóźnienia dla replikacji danych.
- Muszą istnieć połączenia sieciowe umożliwiające produkcję w Ośrodku Zapasowym
- RPO – blisko 0 dla krytycznych danych.
- RTO < 12 godzin

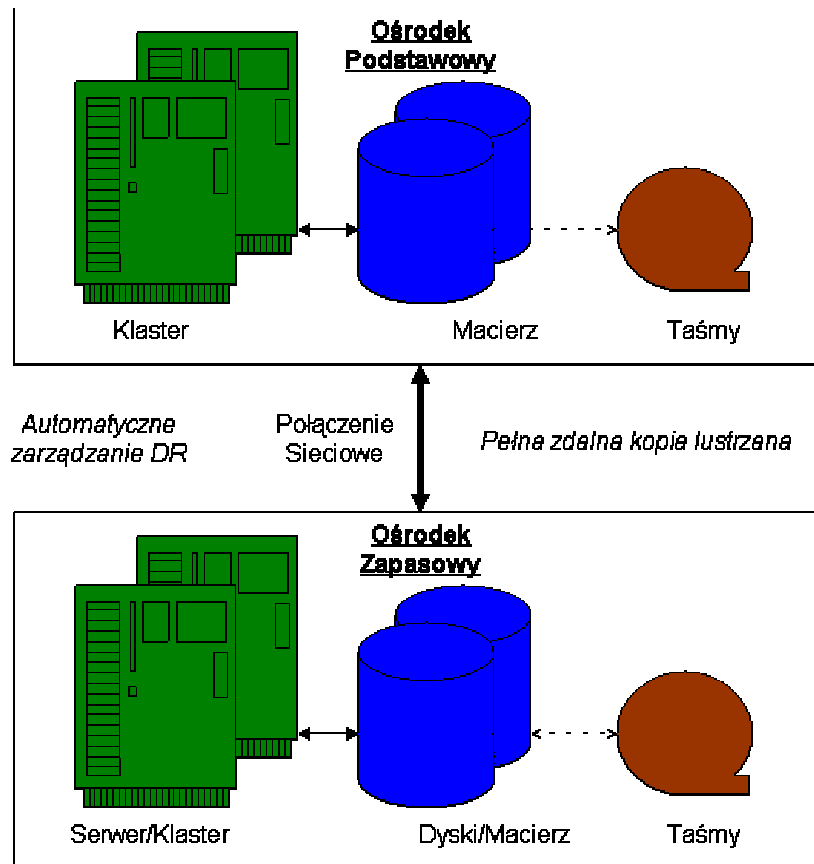
6 – Zero Data Loss (Bez utraty danych)



Rys. 10. Poziom 6

- Najwyższe wymagania *Disaster Recovery*
- Plan Awaryjny jest zdefiniowany, istnieją udokumentowane procedury
- Dane są stale aktualizowane poprzez mechanizm zdalnej kopii lustrzanej
- Odtwarzanie jest bardzo szybkie. Dane są aktualne. Ośrodek Zapasowy może na bieżąco uczestniczyć w obciążeniu produkcyjnym. Wyposażenie i personel Ośrodka są kompletne.
- Czas odtwarzania zwykle wynosi poniżej jednej godziny.
- Musi istnieć połączenie sieciowe pomiędzy Ośrodkami zapewniające nieznaczące opóźnienia dla zdalnej kopii lustrzanej.
- Muszą istnieć połączenia sieciowe umożliwiające produkcję w Ośrodku Zapasowym
- RPO – blisko 0
- RTO < 1 godziny

7 – Automatic site switch (Automatyczne przełączenie)

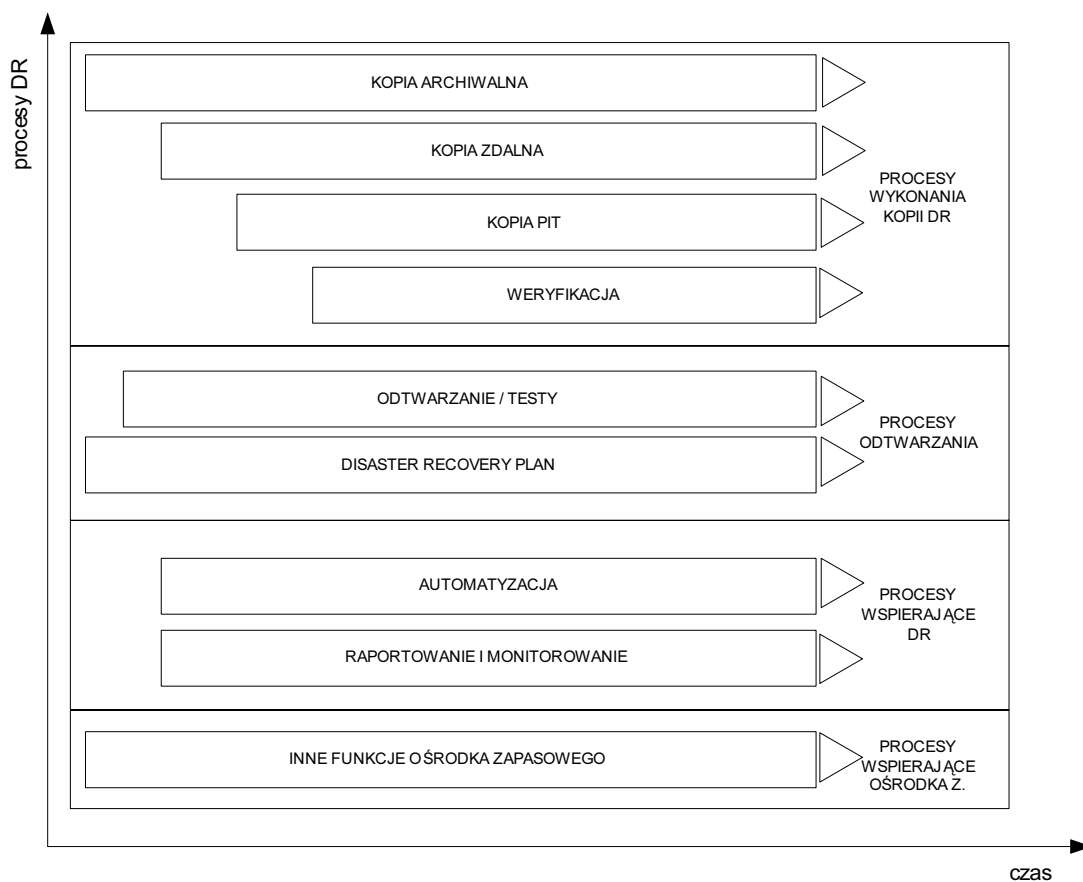


Rys. 11. Poziom 7

- Najwyższe wymagania *Disaster Recovery*
- Plan Awaryjny jest zdefiniowany, istnieją udokumentowane procedury
- Dane są stale aktualizowane poprzez mechanizm zdalnej kopii lustrzanej
- Odtwarzanie jest automatyczne. Dane są aktualne. Ośrodek Zapasowy może na bieżąco uczestniczyć w obciążeniu produkcyjnym. Wyposażenie i personel Ośrodka są kompletne.
- Czas odtwarzania zwykle wynosi poniżej 30 minut.
- Musi istnieć połączenie sieciowe pomiędzy Ośrodkami zapewniające nieznaczące opóźnienia dla zdalnej kopii lustrzanej.
- Muszą istnieć połączenia sieciowe umożliwiające produkcję w Ośrodku Zapasowym
- Muszą być zaimplementowane mechanizmy (oprogramowanie) automatycznego zarządzania DR.
- RPO – blisko 0
- RTO - < 30 minut

3. Implementacja rozwiązania DR

Implementacja rozwiązania *Disaster Recover* realizowana jest poprzez grupy procesów. Zasadniczym procesem, rozpoczynającym wdrożenie i trwającym cały czas jest tworzenie i utrzymanie Planu Awaryjnego. Tam też opisane są zależności pomiędzy procesami oraz procedury wykonawcze. Modularność procesów pozwala na łatwiejszą koordynację zmian i rozwój rozwiązania.



Rys. 12. Implementacja rozwiązania DR

3.1. Procesy Wykonania Kopii DR

Procesy odpowiedzialne za realizację kopii DR wykonywane są cyklicznie w ramach ustalonego harmonogramu. Ten zestaw procesów wdrażany jest jako pierwszy – bez poprawnie wykonanej kopii DR nie ma mowy o odtwarzaniu po katastrofie.

KOPIA ARCHIWALNA – Proces archiwizacji kopii DR na taśmy

KOPIA ZDALNA – Proces tworzenia i utrzymania zdalnej kopii lustrzanej (*secondary*)

KOPIA PIT – Proces realizacji błyskawicznej kopii Point in Time (*tertiary*)

WERYFIKACJA – Proces weryfikacji poprawności kopii DR

Szczególne znaczenie ma proces WERYFIKACJI. Bez tego procesu, nie można być pewnym poprawności odkładanej kopii, a tym samym jej przydatności w przypadku katastrofy. WERYFIKACJA odbywa się z reguły na KOPII PIT. Dzięki temu nie jest zaburzany proces utrzymania KOPII ZDALNEJ. KOPIA PIT (*tertiary*), odkładana i weryfikowana cyklicznie stanowi ochronę przed błędem logicznym w danych, który natychmiast jest przenoszony z produkcji na KOPIĘ ZDALNĄ (*secondary*).

3.2. Procesy Odtwarzania

Procesy odtwarzania realizowane są w następujących przypadkach:

- cykliczne przygotowanie do WERYFIKACJI,
- testy Planu Awaryjnego,
- katastrofa

ODTWARZANIE / TESTY – Proces odtwarzania opisuje czynności niezbędne do podjęcia przetwarzania produkcyjnego w Ośrodku Zapasowym lub przygotowania kopii do WERYFIKACJI

DISASTER RECOVERY PLAN - Podstawowy proces realizacji rozwiązania DR. polegający na przygotowaniu i utrzymaniu Planu Awaryjnego.

Scenariusze odtwarzania po katastrofie muszą być ćwiczone według ustalonego harmonogramu. Niedopuszczalne jest pozostawienie jednokrotnie sprawdzonych procedur „na półkę” z myślą sięgnięcia po nie w przypadku katastrofy. Przyjmuje się, że testy scenariuszy odtwarzania według Planu Awaryjnego powinny być ćwiczone co 6 miesięcy.

3.3. Procesy Wspierające DR

Ta grupa procesów ma za zadanie wspomagać realizację zasadniczych procesów DR (Wykonania Kopii DR i Odtwarzania). Wdrażanie tych procesów może odbywać się stopniowo i nie musi wystartować od początku projektu. Wprowadzenie AUTOMATYZACJI jest niezbędne dla osiągnięcia poziomu 7.

AUTOMATYZACJA – Proces realizujący automatyzację procesów DR

RAPORTOWANIE I MONITOROWANIE - Proces realizujący raportowanie i monitorowanie przebiegu zasadniczych procesów DR

3.4. Procesy Wspierające Ośrodka Zapasowego

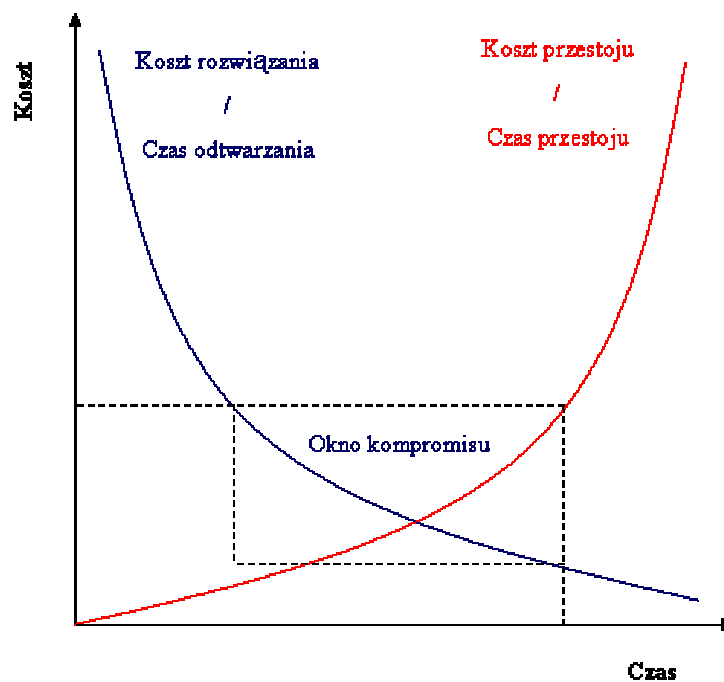
Ośrodek Zapasowy przygotowany do realizacji wysokiego poziomu rozwiązania DR wymaga dużych nakładów finansowych i organizacyjnych. Dlatego istotne jest, aby można go było wykorzystywać również do celów innych niż tylko DR. I tak, zasoby Ośrodka Zapasowego mogą być wykorzystane do:

- przejęcia części obciążenia produkcyjnego,
- testów nowych wersji oprogramowania,
- testów wydajnościowych i innych.

W szczególności, do różnego rodzaju testów nie związanych z DR może być wykorzystana KOPIA PIT (*tertiary*), która stanowi replikę środowiska produkcyjnego (po WERYFIKACJI).

Procesy Wspierające Ośrodka Zapasowego muszą być wdrażane tak, aby nie zaburzyć podstawowych procesów DR. Muszą być też ujęte w Planie Awaryjnym, tak aby na wypadek katastrofy wyłączyć te z nich, które zajmują zasoby potrzebne do przejęcia produkcji przez Ośrodek Zapasowy.

4. Podsumowanie



Rys. 13. Okno kompromisu dla rozwiązania DR

- Im wyższe parametry DR (wyższy poziom rozwiązania), tym większe środki muszą być przeznaczone na realizację projektu.
- Koszty przestoju po katastrofie mogą rosnąć dramatycznie wraz z czasem, który upłynął od katastrofy, a w rezultacie doprowadzić do nieodwracalnych strat.
- Optymalne rozwiązanie *Disaster Recovery* powinno zostać odnalezione w tzw. „oknie kompromisu” pomiędzy dostępnymi środkami na DR a dopuszczalnymi kosztami przestoju

Bibliografia

1. Fire in the Computer Room - What Now?, SG24-4211-01
2. Disaster Recovery Library Data Recovery, GG24-3994
3. International Technical Support Organization Bibliography of Redbooks, GG24-3070. (www.redbooks.ibm.com)