BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 26, 2009

Charakterystyka podstawowych typów zapasowych ośrodków przetwarzania danych

Krzysztof LIDERMAN

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT,
ul. S. Kaliskiego 2, 00–908 Warszawa

STRESZCZENIE: Artykuł zawiera przegląd i charakterystykę podstawowych typów ośrodków zapasowych, ze szczególnym uwzględnieniem przeznaczonych do replikacji danych. Opisano także podstawowe sposoby zwiększania odporności systemu teleinformatycznego i danych na skutki katastrof.

SŁOWA KLUCZOWE: odtworzenie systemu i danych po katastrofie, lokalizacja zapasowa, ciągłość działania, replikacja danych, RTO, RPO, RTA, NRO.

1. Wstęp

Podstawowym zabezpieczeniem przed utratą ciągłości działania, w przypadku katastrofy niszczącej newralgiczne elementy firmy lub organizacji, jest ośrodek zapasowy. Można wyróżnić dwa podstawowe zastosowania ośrodków zapasowych:

1. Zapasowy ośrodek dla danych odtworzeniowych (ang. *alternate storage site*);
2. Zapasowy ośrodek dla prowadzenia biznesowych działań operacyjnych (ang. *alternate processing site*)[1].

Oczywiście jest to podział uproszczony, w praktyce będą też budowane ośrodki zapasowe typu mieszanego, łączące funkcje zapasowego składowania i odtwarzania danych jak i prowadzenia działalności biznesowej polegającej np. na bezpośredniej obsłudze klientów. Co więcej, pojęcie „centrum zapasowe" dla

[1] Szczególnym przypadkiem tego typu ośrodka będzie zapasowe *centrum zarządzania kryzysowego*.

konkretnej firmy może w praktyce oznaczać np. zapasowe centrum danych wykorzystywane na zasadach hostingu (por. dalszą część tego opracowania) plus salę gimnastyczną pobliskiej szkoły gminnej do której, w przypadku katastrofy, będą przeniesieni zdolni do pracy pracownicy i sprzęt biurowy aby kontynuować obsługę klientów.

W zależności od stopnia przygotowania ośrodka zapasowego do przejęcia działalności produkcyjnej (operacyjnej) można wyróżnić typy przedstawione w tabeli 1. Od strony organizacyjnej, ośrodek zapasowy może być:

1) typu „wymiana usług" z inną firmą/organizacją o podobnym profilu działalności;
2) własnym, firmowym ośrodkiem zapasowym;
3) ośrodkiem dzierżawionym na zasadach hostingu[2] lub kolokacji[3] (ośrodek zapasowy dla danych odtworzeniowych).

Tab. 1. Charakterystyka typów ośrodków zapasowych [14]

Typ	Koszty	Wyposażenie w sprzęt	Wyposażenie w środki łączności	Czas przygotowania do działania	Lokalizacja
Zimny (ang. Cold Site)	Niskie	Brak	Brak	Długi	Ustalona
Ciepły (ang. Warm Site)	Średnie	Częściowe	Częściowe lub pełne	Średni	Ustalona
Gorący (ang. Hot Site)	Średnie/ wysokie	Pełne	Pełne	Krótki	Ustalona
Lustrzany (ang. Mirrored Site)	Wysokie	Pełne	Pełne	Pomijalny	Ustalona
Mobilny (ang. Mobile Site)	Wysokie	Zależne od wcześniejszych ustaleń	Zależne od wcześniejszych ustaleń	Zależny od stopnia wstępnego wyposażenia	Nieustalona

[2] Hosting – realizacja usługi (np. składowania danych) przez dostawcę usługi na jego zasobach sprzętowych i programowych, w jego centrum danych.
[3] Kolokacja – usługa polegająca na wynajęciu miejsca w centrum danych dostawcy usługi i umieszczeniu w nim własnego sprzętu komputerowego.

Niniejsze opracowanie dotyczy przede wszystkim ośrodków z ww. grupy pierwszej i skupia się na odtwarzaniu danych niezbędnych do kontynuowania działalności biznesowej. Z badań przeprowadzonych przez amerykańskie miesięczniki CIO i CSO w 2004 roku wspólnie z Pricewaterhouse Coopers na grupie ponad 8 tys. firm z 62 krajów świata wynika, że wiodące firmy przeznaczają na szeroko pojęte bezpieczeństwo nawet do 14% budżetów IT [3]. Czasami duża część tego budżetu jest wydatkowana na organizację zapasowego centrum danych. Należy mieć jednak na uwadze, że własne centrum zapasowe jest przydatne tylko organizacji, która musi pracować bez przerw, dysponuje bardzo dużą ilością zasobów i nie może, ze względów formalnych, pozwolić na dostęp do zasobów informacyjnych firmie trzeciej. W innych przypadkach ekonomiczniejszy może być outsourcing [2].

Zabezpieczenie w postaci ośrodka zapasowego ma dawać gwarancję ciągłości działalności biznesowej na wypadek katastrofy lub poważnej awarii systemu teleinformatycznego, wspierającego kluczowe procesy biznesowe, w podstawowej siedzibie firmy lub podstawowym ośrodku obliczeniowym. Przy rozważaniach nt. ciągłości działania, pomocna może być klasyfikacja procesów według *Harvard Research Group*:

1. **Fault Tolerant** (tolerujące błędy, AE-4) – funkcje wymagające ciągłego przetwarzania, przy których każde zakłócenie staje się widoczne dla użytkownika. Oznaczają niedopuszczalność przerw w pracy, brak utraconych transakcji, brak obniżonej jakości działania i ciągłość działania 24x7 (24 godzin dziennie, 7 dni w tygodniu).
2. **Fault Resilient** (odporne na błędy, AE-3) – funkcje wymagające ciągłego przetwarzania podczas określonych godzin lub przez większość godzin w ciągu dnia i większość dni w roku – oznacza to ciągłość pracy dla użytkownika, lecz dopuszczalne jest powtórzenie aktualnej transakcji i pewne obniżenie jakości działania.
3. **High Availability** (wysoka dostępność, AE-2) – funkcje wymagające ciągłego przetwarzania podczas określonych godzin lub przez większość godzin w ciągu dnia i większość dni w roku, ale dopuszczające minimalne przerwy w działaniu – oznacza to możliwość przerwania pracy użytkownika, ewentualnie z koniecznością odtworzenia transakcji i obniżeniem jakości działania.
4. **Highly Reliable** (wysoka niezawodność, AE-1) – funkcje dopuszczające przerwanie pracy pod warunkiem zachowania integralności danych – z punktu widzenia użytkownika następuje niekontrolowana przerwa w pracy, lecz zachowywana jest integralność danych.
5. **Conventional** (zwykłe, AE-0) – funkcje mogą być przerwane, a integralność danych nie jest istotna – dane mogą zostać utracone lub zniekształcone.

Pojęcie katastrofy jest pojęciem niejednoznacznym. Patrząc od strony systemów teleinformatycznych katastrofa następuje wtedy, kiedy z jakiegoś powodu (awarii, klęski żywiołowej itp.) przerwa w pracy systemu przekracza dopuszczalny czas. Do wyznaczania tego czasu, jak również wskazania środków zaradczych, niezbędna jest analiza ryzyka [5]. Jej podstawowym elementem w przypadku analizy zdarzeń katastrofalnych jest tzw. analiza skutków (BIA – *Business Impact Analysis*), gdzie zidentyfikowanym zdarzeniom z kategorii „katastrofa" przypisuje się potencjalne skutki (por. tab. 2) i częstość ich zajścia. W przypadku „klasycznych" systemów przetwarzania danych potencjalne skutki będą należały do kategorii 2, 4, 5, w przypadku tzw. systemów przemysłowych obejmują również kategorie 1 i 3.

Tab. 2. Przykładowe definicje skutków (ang. *impact*) według zaleceń ISA-TR99.00.02

Lp.	Kategoria skutków	Szkody niskie	Szkody średnie	Szkody wysokie
1	**Obrażenia u ludzi**	Urazy i stłuczenia wymagające podstawowej pomocy lekarskiej	Urazy i stłuczenia wymagające hospitalizacji	Utrata życia lub kończyn
2	**Straty finansowe**	Rzędu 1000$	Rzędu 100 000$	Rzędu milionów $
3	**Szkody w otoczeniu**	Szkody krótkoterminowe	Szkody długoterminowe	Szkody długoterminowe i poza firmowym środowiskiem
4	**Przerwa w działalności operacyjnej**	Minuty	Dni	Tygodnie
5	**Wizerunek publiczny firmy**	Szkody krótkoterminowe	Szkody długoterminowe	Całkowita utrata zaufania publicznego

2. Zapasowa lokalizacja danych odtworzeniowych

Podstawowym zabezpieczeniem przed utratą informacji (danych), spowodowaną katastrofą, jest wykonywanie kopii zapasowych (inna nazwa: kopia bezpieczeństwa). Proces wykonywania kopii zapasowych potocznie nazywany jest *backupem*. W jego wyniku otrzymuje się kopię zapasową, która może być w przyszłości użyta do odtworzenia (ang. *recovery*) danych i systemu. Ponieważ zwykle potrzeba taka zachodzi po katastrofie, proces takiego odtworzenia jest elementem działań nazywanych w języku angielskim *disaster recovery*, a opis organizacji tego procesu jest ujęty w planie odtworzenia

systemu i danych po katastrofie (ang. *disaster recovery plan*)[4].

Należy zauważyć, że chociaż proces wykonywania kopii zapasowych i proces odtworzenia są odrębnymi, rozdzielonymi w czasie procesami, to wspólnie mają zapewnić osiągnięcie następujących celów:

1. Zminimalizować ilość danych utraconych z powodu katastrofy,
2. Zminimalizować czas niedostępności usług informatycznych/informacji spowodowany realizacją procedur awaryjnych i odtworzeniowych,
3. Zminimalizować koszty procesu wykonywania kopii zapasowej i procesu odtwarzania, przy zapewnieniu osiągnięcia dwóch ww. celów.

2.1. Podstawowe parametry określające działania odtworzeniowe

Podstawowe parametry określające działania odtworzeniowe, to:

1. *Recovery Time Objective* (RTO) – parametr ten określa maksymalny, możliwy do zaakceptowania przez kierownictwo firmy ze względu na ponoszone straty, czas pracy firmy lub organizacji bez możliwości korzystania z usług całości lub części systemu informatycznego. Jest to jednocześnie maksymalny, szacowany czas niezbędny do odtworzenia systemu. RTO jest ustalany podczas analizy ryzyka (BIA – Business Impact Analysis) i podlega zatwierdzeniu przez naczelne kierownictwo firmy/organizacji. Odzwierciedla biznesowe spojrzenie na skutki katastrofy przez pryzmat przerwania głównych procesów biznesowych. RTO powinno się określić dla każdego wyspecyfikowanego w „Planie odtwarzania działania systemów teleinformatycznych ...” systemu teleinformatycznego, w odniesieniu do każdego kluczowego elementu programowego lub sprzętowego, usługi oraz danych [4].
2. *Recovery Point Objective* (RPO) – parametr ten określa „akceptowalne straty w danych” (aktualność danych odtworzonych po katastrofie) mierzone czasem od ostatniej kopii zapasowej do chwili katastrofy.

Przykład

Dane odtworzone z kopii wykonywanej codziennie o ustalonej godzinie mają RPO=24godz. Jeżeli np. RPO=2godz. (czyli kopia zapasowa powinna być wykonywana co dwie godziny), kopia była wykonana o godzinie 9:00, a katastrofa wydarzyła się o 10:59, to zostaną utracone dane wprowadzone i przetwarzane pomiędzy 9:00 a 10:59. Po odtworzeniu, działanie systemu będzie kontynuowane od stanu z godziny 9:00. Dane utracone muszą być odzyskane w inny sposób, np. ręcznie z dokumentacji papierowej.

[4] Niestety, w języku polskim nie ma jednolitego, ogólnie uznawanego i stosowanego nazewnictwa w dziedzinie zapewniania ciągłości działania. Dlatego w niniejszym opracowaniu obok nazw polskich będą podawane terminy angielskie, które są zwykle jednoznacznie interpretowane i stosowane.

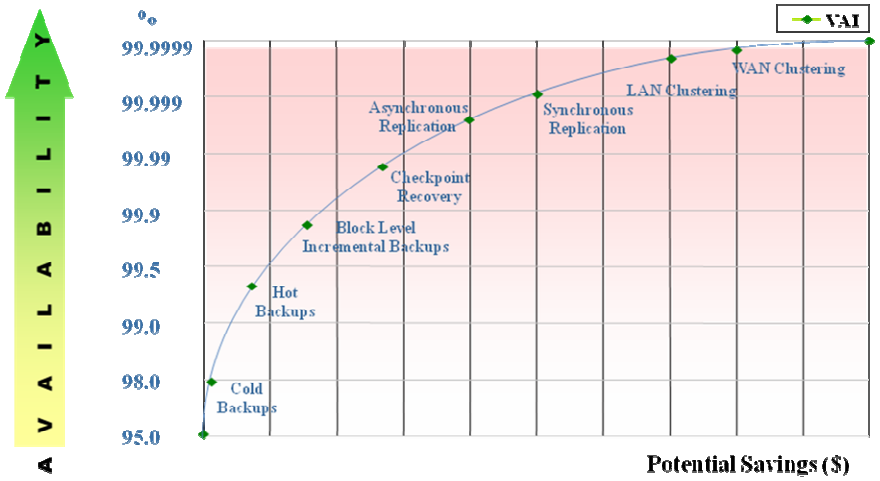
3. *Recovery Time Actual* (RTA) – parametr ten określa, ustalany drogą eksperymentów, czas odtworzenia systemu (RTO był szacowany podczas analizy ryzyka). Powinna być spełniona zależność RTA ≤ RTO.
4. *Network Recovery Objective* (NRO) – parametr ten określa czas niezbędny do odtworzenia połączeń sieciowych poprzez odbudowę połączeń utraconych lub przekierowanie strumienia danych do innych sieci. Na NRO składają się czasy:
   – odtwarzania,
   – niezbędne do wznowienia przetwarzania,
   – niezbędne do osiągnięcia docelowego, wymaganego poziomu usług.
5. *Backup Window Objective* (BWO) – parametr ten określa wymaganą długość przerwy w przetwarzaniu danych, niezbędną do wykonania kopi zapasowej.
6. *Maximum Data Loss* (MDL) – parametr ten określa maksymalną wielkość utraconych danych z uwzględnieniem dodatkowych możliwości odtwarzania (logi transakcji, wprowadzenie dokumentów papierowych itp.).

W tabeli 3 pokazano jak, w kontekście konkretnej klasy systemu teleinformatycznego, poziom dostępności podawany zwykle w procentach, przekłada się na faktyczną ilość godzin niedostępności usług. W nieco inny sposób, tym razem w kontekście stosowanych metod odtworzeniowych, zaprezentowano to na rys. 1. Systemy takie, jak wyspecyfikowane w tab. 3, budowane są w celu zapewnienia świadczenia przez taki system usług na określonym (najczęściej procentowo, tak jak w tabeli), gwarantowanym poziomie.

Tab. 3. Dostępność systemu a czasy przestoju (*źródło - Gartner Group* [16])

Typ systemu	% dostępności	Przestój/rok
Zwykły	99.5%	43.8 godz.
O wysokiej dostępności	99.9%	8,75 godz.
Systemy klastrowe	99.99%	53 min
Systemy odporne na błędy	99.999%	5min.
Z replikacją do Centrum Zapasowego	100%	0 min.[5]

[5] Oczywiście przy założeniu, że nie zostanie zniszczony również ośrodek zapasowy.



Rys. 1. Związki pomiędzy wymaganym poziomem dostępności, rozwiązaniami technicznymi i kosztami (*źródło - Gartner Group* [16])

Informacje o dopuszczalnych, dla konkretnych systemów teleinformatycznych i ich elementów, czasach niedostępności (czyli RTA) można przedstawić np. tak jak w tabeli 4. Taki sposób prezentacji pozwala w szybki sposób zidentyfikować:

- elementy systemu kluczowe pod względem dopuszczalnego czasu odtwarzania działania,
- dopuszczalny czas odtwarzania działania konkretnego elementu,
- związane z tym elementem usługi,
- fakt zajścia zdarzenia kryzysowego[6].

Dla przypadku utraty możliwości działania niektórych elementów systemu teleinformatycznego należy oszacować możliwości pracy tego systemu w trybie ograniczonym, w szczególności dla każdej aplikacji w systemie należy:

- określić minimalne zapotrzebowanie na zasoby systemowe, zakładając utratę możliwości wykonywania niektórych funkcji;
- ustalić, pisemnie zatwierdzony przez odpowiednie kierownictwo, priorytet aplikacji;
- spisać procedurę przejścia w tryb pracy ograniczonej z podaniem, jakie funkcje będą tracone;

[6] Fakt zajścia **zdarzenia kryzysowego** nie musi oznaczać wystąpienia **sytuacji kryzysowej** – przy dobrze opracowanych planach awaryjnych, przedsięwzięcia kryzysowe powinny umożliwić przywrócenie działania **przed** upływem dopuszczalnego czasu niedostępności elementu/usługi.

– rozpoznać możliwość zastąpienia utraconych funkcji np. poprzez ich ręczne wykonanie. Dla tego przypadku należy oszacować zapotrzebowanie na niezbędne środki (ludzie, formularze papierowe, kserokopiarki itd.) i utrzymywać takie rezerwowe środki, lub opracować procedury ich szybkiego pozyskiwania w sytuacji kryzysowej.

Tab. 4. Specyfikacja elementów systemu teleinformatycznego i związane z nimi dopuszczalne czasy odtwarzania działania (*przykład*)

System teleinformatyczny	Element systemu teleinformatycznego	Usługa	Dopuszczalny czas niedostępności
SAP/R3	serwer produkcyjny	lista płac	6 godzin
		gospodarka magazynowa	3 godziny
	biblioteka taśmowa	kopie zapasowe	12 godzin
	drukarka sieciowa	lista płac	3 dni robocze
		faktury	3 dni robocze
...	...	...	...
LAN BIURO	serwer plików	oprogramowanie biurowe_1	1 dzień roboczy
		oprogramowanie biurowe_2	2 dni robocze
	PC	wprowadzanie danych	12 godzin
...	...	…	...

Przy opracowywaniu planów i procedur przechodzenia w tryb pracy ograniczonej należy oszacować możliwości zastąpienia utraconych funkcji i zasobów. W pierwszej kolejności należy rozpatrzyć możliwości wewnętrznego, tj. w ramach dotkniętej kryzysem firmy, zastąpienia utraconych funkcji i zasobów (np. poprzez przeniesienie zadań na serwer szkoleniowy w przypadku awarii serwera produkcyjnego).

Możliwości zewnętrzne powinny być brane pod uwagę dopiero wtedy, gdy zasoby wewnętrzne nie zapewniają wymagań operacyjnych lub rozwiązania takie nie są pożądane z ekonomicznego punktu widzenia. Przy rozpoznawaniu możliwości zastępowania utraconych funkcji i zasobów należy pamiętać również o infrastrukturze, np. pomieszczeniach biurowych.

Szczegóły konstrukcji planów zapewniania ciągłości działania są opisane w dwóch częściach normy [10], [11] opublikowanej przez Brytyjski Instytut Standaryzacji. Pewne wskazówki można też znaleźć w normach ISO/IEC [8], [9]. Warte polecenia są również publikacje w *Disaster Recovery Journal* [2].

2.2. Metody przechowywania danych

Przechowywanie danych uwzględniające minimalizację ich utraty w przypadku zdarzeń katastrofalnych, wymaga przeanalizowania zarówno organizacji dyskowych nośników danych zapewniających bieżącą działalność operacyjną (rozdz. 2.2.1) jak i organizacji dostępnej przestrzeni dyskowej w bardziej złożone struktury (rozdz. 2.2.2). Analiza taka stanowi podstawę do dalszych rozważań nt. architektur (rozdz. 2.3) zapewniających wymagany poziom dostępności danych, gdzie elementami takiej architektury są metody przechowywania danych, sposób przesyłania/przechowywania danych oraz zastosowane zabezpieczenia gwarantujące ich tajność, integralność i dostępność.

2.2.1. Macierze dyskowe typu RAID

Macierze dyskowe typ RAID (nazwa jest akronimem ze słów: *Redundant Array of Inexpensive Disks* – po polsku: *nadmiarowa matryca niedrogich dysków*) są stosowane w celu zwiększenia pojemności i niezawodności podsystemu dyskowego komputera. Macierz ze strony jednostki centralnej jest widziana jako jeden dysk. Początkowo zdefiniowano pięć poziomów (architektur). Do tych początkowych pięciu, producenci dodali jeszcze poziom 0, 6 i 7. Podstawowe poziomy RAID to:

– *RAID_1*
  Dyski są łączone w pary zawierające dokładnie takie same informacje. Możliwe warianty:
  - dyski lustrzane (ang. *mirroring*) – gdy dwa dyski współpracują z jednym sterownikiem sprzętowym;
  - dyski zdublowane (ang. *duplexing*) – gdy każdy dysk ma niezależny sterownik sprzętowy.

– *RAID_2*

  Bajt danych jest zapisywany na 8-miu dyskach (każdy bit na innym dysku). Dodatkowo na trzech dyskach są zapisywane 3 bity nadmiarowe (dla każdego bajtu), ponieważ do zidentyfikowania przekłamań i odtworzenia poprawnej informacji stosuje się tzw. kod Hamminga.

– *RAID_3*

  Kolejne bajty danych są zapisywane na kolejnych dyskach (zwykle 2-4), a na dysku dodatkowym – wartość funkcji logicznej XOR zapisywanej informacji.

– *RAID_4*

  Kolejne sektory danych są zapisywane na kolejnych dyskach (zwykle 2-4), a na dysku dodatkowym – suma modulo 2 zapisywanej informacji.

– *RAID_5*

  W odróżnieniu od RAID_4 informacja kontrolna jest zapisywana na dowolnym z dysków macierzy (brak wydzielonego dysku z informacją kontrolną).

Macierze wszystkich poziomów potrafią kontynuować pracę w przypadku awarii jednego dysku. Oprócz opisanych, podstawowych poziomów RAID, można także spotkać następujące mieszane, łączące różne cechy podstawowych poziomów, konstrukcje:

– *RAID_0* – jest to macierz dyskowa, ale nie ma zapisanej informacji nadmiarowej. Dane rozrzucone są równomiernie w pasmach (wielokrotnościach bloku) po wszystkich dyskach wchodzących w skład macierzy.
– *RAID_0+1* – (*stripping and mirroring;* oznaczany czasem jako RAID 10) polega na dublowaniu nie całych dysków, lecz pojedynczych pasm, dzięki czemu może występować tu nieparzysta liczba dysków.
– *RAID_6* – jest rozwiązaniem niestandardowym i jego definicja zmienia się w zależności od dostawcy. Może to być lustrzany układ dwu zestawów RAID_0. Inny sposób polega na dodaniu do RAID_3, RAID_4 lub RAID_5 dodatkowych danych kontrolnych.
– *RAID_7* – występuje w dwóch wariantach. Pierwszy wariant polega na połączeniu RAID_0, RAID_3 lub RAID_5 z tzw. funkcją *hot spare* („gorący zapas" w postaci dodatkowego dysku), drugi natomiast to system dyskowy dysponujący własnym systemem operacyjnym i oprogramowaniem sterującym i kontrolnym.

Zastosowanie macierzy RAID nie zastępuje kopii bezpieczeństwa (zapasowych), ponieważ nie chroni przed:

– fizycznym zniszczeniem serwera z podłączoną macierzą RAID w wyniku katastrofy – jeśli dane nie będą znajdowały się w innym, oddalonym fizycznie miejscu, to np. pożar lub zalanie serwera może doprowadzić do ich utraty;
– awarią sterownika dysków – uszkodzenie sprzętowego sterownika realizującego funkcję RAID może uszkodzić wszystkie dane przechowywane na dyskach, bez względu na wykorzystywany tryb RAID;
– błędami ludzkimi – błędne usunięcie plików zostanie rozpropagowane na wszystkie dyski wchodzące w skład macierzy (RAID przechowuje zawsze aktualną kopię plików i nie daje możliwości odwołania się do wersji plików sprzed kilku dni czy tygodni).

2.2.2. Organizacja przestrzeni dyskowej

Przy planowaniu wdrożenia pamięci masowych (macierz dyskowa, serwer pamięci optycznych, biblioteka taśmowa itp.) w firmie, należy określić sposób udostępnienia tych zasobów. Można wyróżnić trzy podstawowe sposoby udostępniania (por. także tab. 5):

Tab. 5. Różnice pomiędzy rozwiązaniami typu NAS i SAN

RÓŻNICE POMIĘDZY ROZWIĄZANIAMI	
NAS	SAN
Praktycznie wszystkie komputery podłączone do LAN (lub mające dostęp z WAN) mogą (używając protokołów NFS, CIFS, http) podłączyć się do NAS i wymieniać pliki.	Tylko urządzenia klasy serwera z SCSI Fibre Channel mogą się podłączyć do SAN. Fibre Channel ogranicza odległość połączeń do ok. 10 km.
NAS identyfikuje dane poprzez nazwy plików i offset bajtowy, przesyła pliki danych lub pliki z meta danymi (właściciel pliku, przywileje, data utworzenia itp.) i zapewnia ochronę danych (np. uwierzytelnianie użytkowników itp.).	SAN adresuje dane poprzez numer bloku dyskowego i przesyła nieprzetworzone (raw) bloki dyskowe.
NAS umożliwia wymianę danych pomiędzy różniącymi się systemami operacyjnymi, jak Unix i NT.	Wymiana danych jest zależna od systemu operacyjnego i nie może zachodzić pomiędzy różnymi systemami operacyjnymi.
System plików jest zarządzany przez urządzenie NAS.	System plików jest zarządzany przez serwer.
Backupy i kopie lustrzane są wykonywane jako pliki a nie bloki, aby zaoszczędzić pasmo i czas.	Backup i kopia lustrzana są wykonywane jako kopia blok po bloku, nawet jeżeli bloki są puste. Dyski na kopie lustrzane muszą mieć pojemność większą niż dyski źródłowe.

1. Podłączanie pamięci masowej bezpośrednio do gromadzącego dane komputera (**DAS**, ang. *Direct Attached Storage*).

   W praktyce są to pamięci dyskowe USB, FireWire, eSATA podłączone bezpośrednio do komputera w sieci oraz urządzenia specjalne, np. macierze dyskowe, podłączane do serwerów lub urządzeń sieciowych za pośrednictwem interfejsu SCSI lub Fibre Channel.

2. Podłączanie pamięci masowych bezpośrednio do sieci Ethernet (**NAS**, ang. *Network Attached Storage*).

   Są to urządzenia nazywane potocznie *dyskami sieciowymi*, które można dołączyć w dowolnym miejscu infrastruktury sieciowej, uzyskując możliwość dostępu do nich z dowolnego miejsca tej infrastruktury i, w zależności od ich skonfigurowania, z sieci publicznej. Urządzenie typu NAS jest niewidoczne dla użytkownika – ma on dostęp do plików przez protokół SMB/FTP, bez bezpośredniego dostępu do zainstalowanych dysków. NAS są często w obudowach typu *rack*, przystosowane do montażu w szafach. Zwykle są to samodzielne i niezależne urządzenia sieciowe, mające wbudowane serwery różnych usług (FTP, WWW, druku, itp.), sterowane i konfigurowane z poziomu przeglądarki internetowej, mogące służyć np. jako urządzenia backupowe.

3. Organizacja pamięci masowych w strukturę sieciową (**SAN**, ang. *Storage Area Network*).

   Na sieć SAN, oprócz urządzeń pamięci masowych, składa się także dodatkowa infrastruktura (okablowanie, karty Host Bus Adapter, przełączniki, serwery itp.) oraz odpowiednia jej organizacja w postaci topologii połączeń (z pętlą arbitrażową[7], typu Fabric[8]) oraz wykorzystywanych protokołów. Podstawowe protokoły to iFCP (SANoIP) czyli mapowanie SCSI na Fibre Channel Protocol over IP oraz popularniejszy (tańszy) iSCSI (ang. *Internet SCSI*) czyli mapowanie SCSI na TCP/IP, umożliwiające wykonywanie operacji wejścia-wyjścia na dysku twardym na odległym komputerze za pomocą protokołu TCP/IP. Protokół iSCSI umożliwia budowę systemów pamięci masowych SAN przy zastosowaniu macierzy dyskowych SCSI i sieci Ethernet (protokół TCP/IP). Zaletą iSCSI jest możliwość tworzenia rozległych systemów SAN przy wykorzystaniu typowych elementów sieciowych, co ułatwia budowę systemu i zmniejsza jego koszt w porównaniu z klasycznymi rozwiązaniami typu Fibre Channel. Specyfikacja iSCSI określa sposób transformacji równoległych poleceń SCSI na format TCP/IP i na odwrót. Transformacja poleceń może być realizowana zarówno sprzętowo jak i programowo. Pomimo wysokich kosztów i skomplikowanym zarządzaniu, stosowanie rozwiązań typu SAN jest konieczne, gdy ilość przetwarzanych i archiwizowanych danych liczona jest w terabajtach.

[7] FC-AL, ang. *Fibre Channel-Arbitrated Loop* – sieć Fibre Channel z pętlą arbitrażową.
[8] Nazywana też *Point-to-Point*.

2.3. Podstawowe architektury systemów przetwarzania danych zwiększające odporność procesu przetwarzania danych i przechowywania informacji na awarie i katastrofy

Systemy wykonywania kopii zapasowych (backupu), w zależności od zastosowanych rozwiązań organizacyjnych, sprzętowych i programowych, mają różne ograniczenia wpływające na wielkość RTA i RPO. „Klasyczny" backup, wykonywany np. codziennie w nocy lub co kilka godzin, nie umożliwia natychmiastowego wznowienia pracy w razie utraty serwera lub nośników, ponieważ:

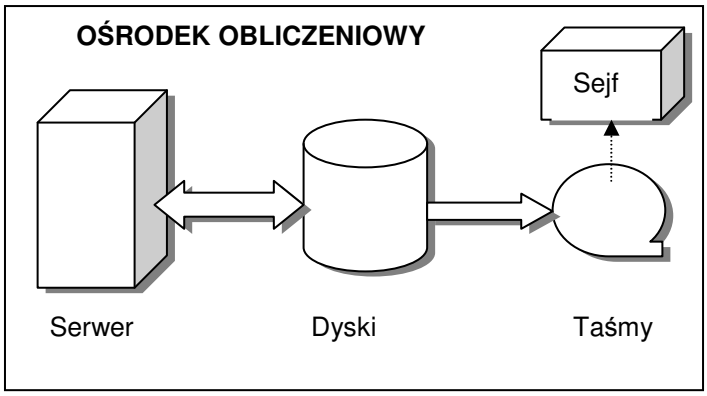
- podczas odtwarzania system nie będzie dostępny dla pracowników lub klientów;
- po odtworzeniu z kopii zapasowej utracimy dane z ostatnich kilku do kilkunastu godzin pracy;
- dodatkowe czynności, związane z analizą strat i opracowaniem sposobu odzyskania utraconych danych, mogą zająć kilka dni.

W roku 1992 organizacja użytkowników SHARE w porozumieniu z IBM zdefiniowała zestaw poziomów rozwiązania problemu Disaster Recovery[9], czyli rozwiązania (architektury) zwiększające odporność procesu przetwarzania danych i przechowywania informacji na awarie i katastrofy. Podstawowymi parametrami, którymi operuje się w tej klasyfikacji są RTO i RPO. Dalej zostaną krótko scharakteryzowane poszczególne architektury (poziomy) [7], [15].

Poziom 0 – No off-site data (kopia lokalna składowana na miejscu, rys. 2).

1. Brak planu odtwarzania działania, w szczególności procedur przywracania danych i systemu do stanu sprzed katastrofy/awarii.
2. Brak kopii zapasowej lub jest to kopia taśmowa, przechowywana lokalnie (brak odporności na katastrofy).
3. RTO i RTA nie są określone; przy braku kopii zapasowej odtworzenie danych może nie być możliwe. W praktyce są one bardzo duże, równe czasowi sprowadzenia części (lub odbudowy ośrodka w przypadku np. pożaru lub katastrofy budowlanej) oraz odtworzenia danych z kopii z taśmowych (o ile istnieją) lub w inny sposób.

[9] Poziom 7 (automatyczne przełączanie) został dodany w późniejszych latach.



Rys. 2. Ośrodek obliczeniowy – konfiguracja podstawowa

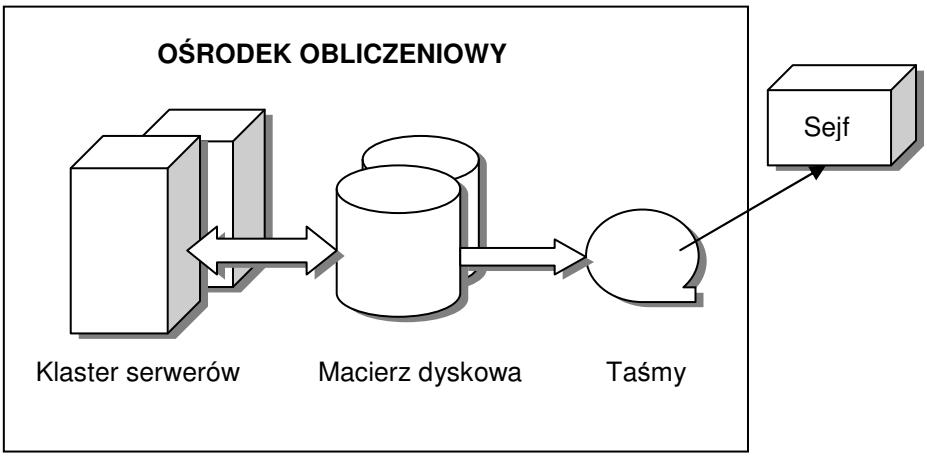
4. RPO – równe częstotliwości wykonywania kopii zapasowej (zwykle 24 godz.).
5. Żaden z elementów systemu nie jest redundantny; awaria któregokolwiek z elementów (serwer, dyski) jest tożsama z katastrofą – przetwarzanie nie może być kontynuowane.

lub:

6. Infrastruktura informatyczna jest nadmiarowa: klaster serwerów (w konfiguracji on-line lub standby) oraz dyski (zwykle macierz dyskowa, por. także rys. 3). Awaria jednego z elementów (serwer, dyski) nie jest tożsama z katastrofą – przetwarzanie może być kontynuowane z wykorzystaniem elementów zdublowanych (ale taka konfiguracja nadal nie jest odporna na katastrofy kończące się zniszczeniem fizycznym ośrodka).

Poziom 1 – Pickup Truck Access Method (PTAM; kopia lokalna składowana zewnętrznie, rys. 3).

1. Jest udokumentowany plan odtwarzania działania, w szczególności procedury przywracania danych i systemu do stanu sprzed katastrofy/awarii.
2. Jest zapasowa, odmiejscowiona (transportowana fizycznie do oddalonego miejsca przechowywania, bez możliwości odtworzenia w nim danych) kopia taśmowa.
3. RTO i RTA słabo określone; w praktyce są one bardzo duże, równe czasowi sprowadzenia części (lub odbudowy ośrodka w przypadku np. pożaru lub katastrofy budowlanej) oraz odtworzenia systemu i danych z kopii taśmowych.

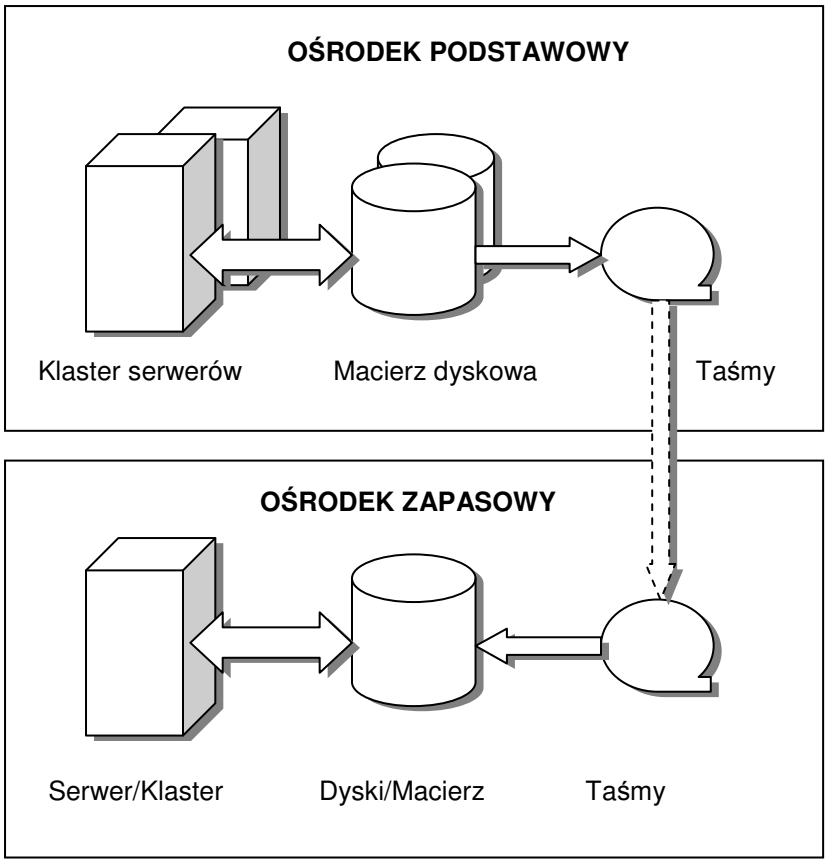


Rys. 3. Ośrodek obliczeniowy – konfiguracja redundantna

4. RPO – równe częstotliwości wykonywania kopii zapasowej (zwykle 24 godz.).
5. Infrastruktura informatyczna zwykle jest nadmiarowa: klaster serwerów (w konfiguracji on-line lub standby) oraz dyski (zwykle macierz dyskowa). Awaria, jednego z elementów (serwer, dyski) nie jest tożsama z katastrofą – przetwarzanie może być kontynuowane z wykorzystaniem elementów zdublowanych (ale taka konfiguracja nadal nie jest odporna na katastrofy kończące się zniszczeniem fizycznym ośrodka).

Poziom 2 – PTAM + hot site (kopia lokalna + Ośrodek Zapasowy, rys. 4).

1. Jest udokumentowany plan odtwarzania działania, w szczególności procedury przywracania danych i systemu do stanu sprzed katastrofy/awarii.
2. Jest zapasowa, odmiejscowiona (transportowana fizycznie do ośrodka zapasowego) kopia taśmowa.
3. RTO i RTA słabo określone – w praktyce zależą od stopnia gotowości ośrodka zapasowego (por. tab. 1), np. moc obliczeniowa jest obliczona tylko dla przetwarzania krytycznego; w przypadku katastrofy infrastruktura ośrodka zapasowego jest stopniowo rozbudowywana.
4. RPO – równe częstotliwości wykonywania kopii zapasowej (zwykle 24 godz.).
5. Infrastruktura informatyczna ośrodka podstawowego zwykle jest nadmiarowa.

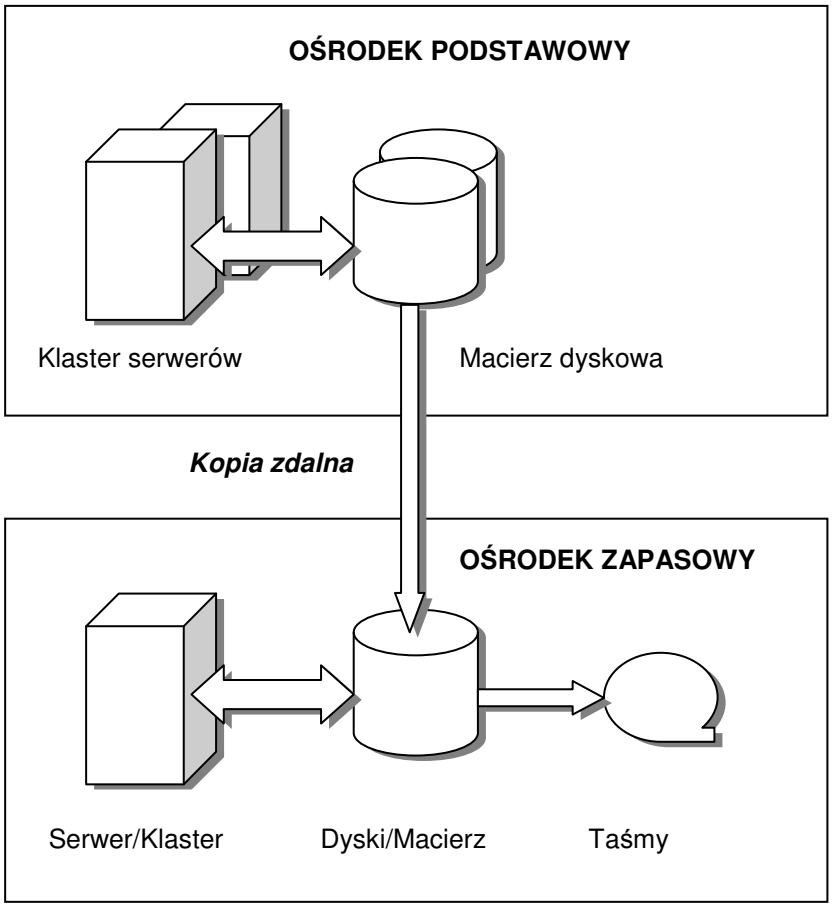


Rys. 4. Ośrodek Obliczeniowy Podstawowy z Ośrodkiem Zapasowym (dane przenoszone na taśmach)

Poziom 3 – Electronic vaulting (kopia zdalna w Ośrodku Zapasowym, rys. 5).

1. Jest udokumentowany plan odtwarzania działania, w szczególności procedury przywracania danych i systemu do stanu sprzed katastrofy/awarii.
2. Dane są zabezpieczone bezpośrednią kopią zdalną w ośrodku zapasowym, który musi mieć odpowiednią przestrzeń dyskową do jej odbioru. Ze względów archiwalnych (możliwości powrotu do kopii starszej niż ostatnia) zaleca się wykonanie kopii taśmowej w ośrodku zapasowym. Metoda PTAM może być wykorzystana jako dodatkowe zabezpieczenie.
3. Musi istnieć połączenie sieciowe pomiędzy ośrodkami zapewniające wykonanie kopii zdalnej.

4. RTO i RTA – średnie, odtwarzanie jest szybkie.
5. RPO – równe częstotliwości wykonywania kopii zapasowej (zwykle 24 godz.).
6. Infrastruktura informatyczna ośrodka podstawowego zwykle jest nadmiarowa.



Rys. 5. Ośrodek Obliczeniowy Podstawowy z Ośrodkiem Zapasowym (dane kopiowane bezpośrednio na dysk w ośrodku zapasowym)

Poziom 4 – Active Secondary Site (aktywny ośrodek zapasowy)

1. Jest udokumentowany plan odtwarzania działania, w szczególności procedury przywracania danych i systemu do stanu sprzed katastrofy/awarii.

2. Dane są zabezpieczone bezpośrednią kopią zdalną w ośrodku zapasowym, który musi mieć odpowiednią przestrzeń dyskową do jej odbioru. Ze względów archiwalnych (możliwości powrotu do kopii starszej niż ostatnia) zaleca się wykonanie kopii taśmowej w ośrodku zapasowym. Metoda PTAM może być wykorzystana jako dodatkowe zabezpieczenie.
3. Musi istnieć połączenie sieciowe pomiędzy ośrodkami zapewniające wykonanie kopii zdalnej.
4. Ośrodek zapasowy może na bieżąco uczestniczyć w obciążeniu produkcyjnym. Wyposażenie i personel ośrodka są kompletne, odpowiadające wyposażeniu ośrodka podstawowego. Muszą istnieć połączenia sieciowe umożliwiające działalność biznesową w ośrodku zapasowym
5. RTO i RTA – małe, odtwarzanie jest szybkie (zwykle poniżej 24 godzin).
6. RPO – równe częstotliwości wykonywania kopii zapasowej (zwykle 24 godz.).
7. Infrastruktura informatyczna ośrodka podstawowego zwykle jest nadmiarowa.

Poziom 5 – Two-site two-phase commit (zapis jednoczesny)

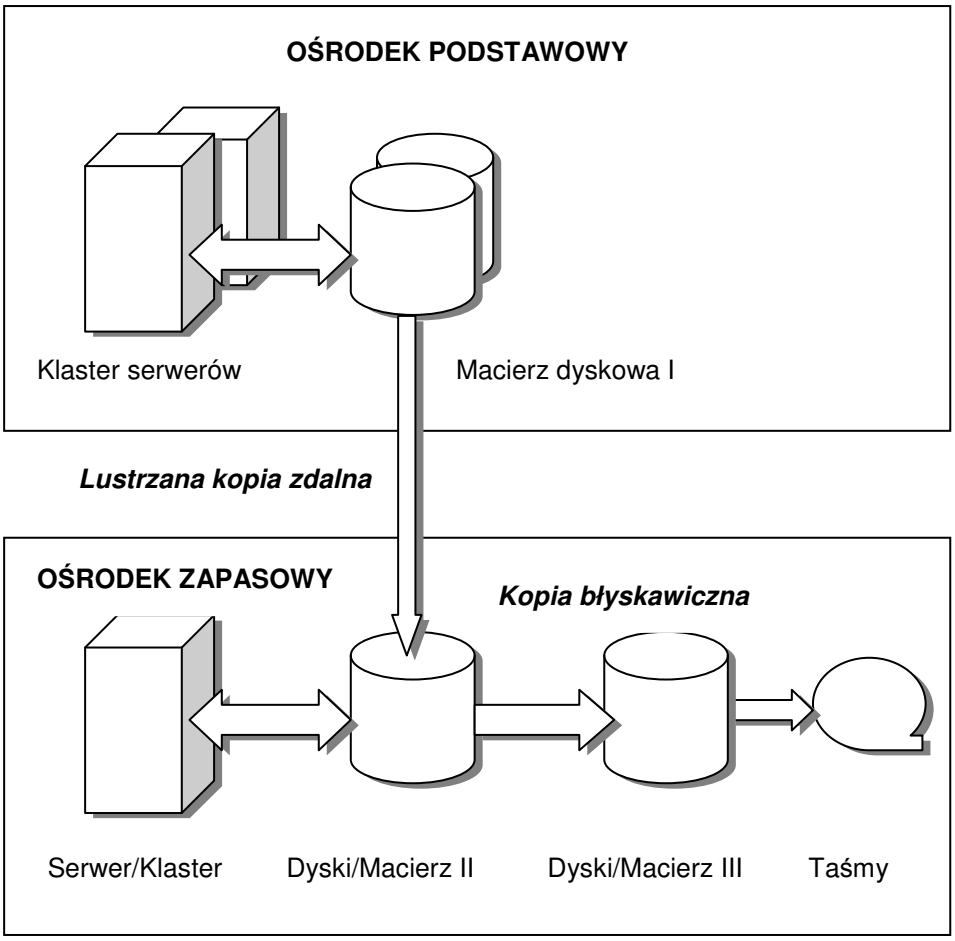
1. Jest udokumentowany plan odtwarzania działania, w szczególności procedury przywracania danych i systemu do stanu sprzed katastrofy/awarii.
2. Dane (całość lub tylko krytyczne) są zabezpieczone w ośrodku zapasowym poprzez mechanizm replikacji lub zapisu jednoczesnego. Ze względów archiwalnych (możliwości powrotu do kopii starszej niż ostatnia) zaleca się wykonanie kopii taśmowej w ośrodku zapasowym. Metoda PTAM może być wykorzystana jako dodatkowe zabezpieczenie.
3. Musi istnieć połączenie sieciowe pomiędzy ośrodkami zapewniające minimalne opóźnienia dla replikacji danych.
4. Ośrodek zapasowy może na bieżąco uczestniczyć w obciążeniu produkcyjnym. Wyposażenie i personel ośrodka są kompletne, odpowiadające wyposażeniu ośrodka podstawowego. Muszą istnieć połączenia sieciowe umożliwiające działalność biznesową w ośrodku zapasowym
5. RTO i RTA – małe, odtwarzanie jest szybkie (zwykle poniżej 12 godzin).
6. RPO – równe częstotliwości wykonywania kopii zapasowej (bliskie zero dla krytycznych danych.).
7. Infrastruktura informatyczna ośrodków zwykle jest nadmiarowa.

Poziom 6 – Zero Data Loss (bez utraty danych, rys. 6).

1. Jest udokumentowany plan odtwarzania działania, w szczególności procedury przywracania danych i systemu do stanu sprzed katastrofy/awarii.
2. Dane są zabezpieczone w ośrodku zapasowym poprzez wykonanie kopii lustrzanej. Ze względów archiwalnych (możliwości powrotu do kopii starszej niż ostatnia) zaleca się wykonanie kopii taśmowej w ośrodku zapasowym. Metoda PTAM może być wykorzystana jako dodatkowe zabezpieczenie.
3. Musi istnieć połączenie sieciowe pomiędzy ośrodkami zapewniające minimalne opóźnienia dla replikacji danych.
4. Ośrodek zapasowy może na bieżąco uczestniczyć w obciążeniu produkcyjnym. Wyposażenie i personel ośrodka są kompletne, odpowiadające wyposażeniu ośrodka podstawowego. Muszą istnieć połączenia sieciowe umożliwiające działalność biznesową w ośrodku zapasowym
5. RTO i RTA – małe, odtwarzanie jest szybkie (zwykle poniżej 1 godziny).
6. RPO – równe częstotliwości wykonywania kopii zapasowej (bliskie zero dla krytycznych danych.).
7. Infrastruktura informatyczna ośrodków zwykle jest nadmiarowa.

Poziom 7 – Automatic site switch (automatyczne przełączenie).

1. Jest udokumentowany plan odtwarzania działania, w szczególności procedury przywracania danych i systemu do stanu sprzed katastrofy/awarii.
2. Dane są zabezpieczone w ośrodku zapasowym poprzez wykonanie kopii lustrzanej. Ze względów archiwalnych (możliwości powrotu do kopii starszej niż ostatnia) zaleca się wykonanie kopii taśmowej w ośrodku zapasowym. Metoda PTAM może być wykorzystana jako dodatkowe zabezpieczenie.
3. Musi istnieć połączenie sieciowe pomiędzy ośrodkami zapewniające minimalne opóźnienia dla replikacji danych.
4. Muszą być wdrożone mechanizmy automatycznego przełączania przetwarzania.
5. Ośrodek zapasowy może na bieżąco uczestniczyć w obciążeniu produkcyjnym. Wyposażenie i personel ośrodka są kompletne, odpowiadające wyposażeniu ośrodka podstawowego. Muszą istnieć połączenia sieciowe umożliwiające działalność biznesową w ośrodku zapasowym
6. RTO i RTA – bardzo małe, odtwarzanie automatyczne, bardzo szybkie (zwykle poniżej 30 minut).
7. RPO – równe częstotliwości wykonywania kopii zapasowej (bliskie zero dla krytycznych danych.).
8. Infrastruktura informatyczna ośrodków zwykle jest nadmiarowa.



Rys. 6. Ośrodek Obliczeniowy Podstawowy z Ośrodkiem Zapasowym (Split Mirror Backup, struktura 3 – poziomowa)

Dodanie dodatkowego, siódmego poziomu, było spowodowane obserwacją, że posiadanie repliki danych w ośrodku zapasowym zabezpiecza co prawda przed utratą danych, ale w przypadku awarii wymagana jest interwencja administratora, który:

- stwierdzi, że mamy do czynienia z awarią;
- przełączy aplikację na serwer zapasowy;
- przełączy dostęp dla klientów końcowych tak, aby używali serwera zapasowego.

W zależności od tego, kiedy nastąpiła awaria i gdzie akurat był administrator, przełączenie aplikacji (ang. *FailOver*) wraz z potrzebnymi do jej pracy zasobami może zająć nawet do kilku godzin. Proces ten można w pełni automatyzować poprzez:

- aktywne monitorowanie serwera (poprawność pracy i dostępność zasobów dyskowych, sieciowych itp.);
- aktywne monitorowanie aplikacji (obecność procesów, czas odpowiedzi, możliwość zalogowania się);
- automatyczny restart aplikacji w środowisku zapasowym (z aktualną repliką danych) w przypadku awarii serwera głównego;
- automatyczne przekonfigurowanie dostępu dla klientów końcowych (zmiana w DNS, zarządzanie wirtualnym adresem IP).

3. Charakterystyka wybranych metod wykonywania kopii zapasowych

Metoda *Split Mirror Backup* (SMB) jest rozwinięciem koncepcji kopii zdalnej, stosowanym zwykle dla instalacji terabajtowych które muszą być dostępne 24/7 – zamiast wykonywać pełną kopię zdalną w określonym cyklu, utrzymuje się w ośrodku zapasowym zdalną kopię lustrzaną dysków produkcyjnych, czyli po stronie ośrodka zapasowego jest cały czas aktualna (dokładniej: prawie aktualna) kopia danych z ośrodka podstawowego. Co pewien czas połączenie jest przerywane (ang. *split mirror*) w celu cyklicznego wykonania, zwykle na taśmy, kopii spójnego obrazu danych, koniecznego co najmniej z dwóch powodów:

1) błąd logiczny w danych produkcyjnych natychmiast propaguje się poprzez kopię lustrzaną do ośrodka zapasowego,
2) jeżeli wystąpi np. stopniowe uleganie awarii kolejnych dysków produkcyjnych (ang. *rolling disaster*), to kopia lustrzana w ośrodku zapasowym będzie niespójna i może nie być możliwe przywrócenie jej spójności.

Zdalna kopia lustrzana ma następujące cechy [6]:

- z reguły jest wspierana sprzętowo,
- ma fazę kopiowania obrazu danych (w tym czasie przetwarzanie powinno być wstrzymane),
- dostępna jest funkcja „zamrożenia" (*split mirror*) – zdalna kopia przestaje być aktualizowana, uzyskujemy spójny obraz na dany moment,

- po zamrożeniu następuje resynchronizacja – „delta zmian" z ośrodka podstawowego jest „doganiana" przez ośrodek zapasowy.

Najprostszym wariantem wykonania kopii typu *split mirror backup* jest struktura dwupoziomowa (jak na rys. 5):

- dyski w ośrodku podstawowym nazywamy dyskami źródłowymi (*primary volumes*);
- dyski w ośrodku zapasowym nazywamy dyskami docelowymi (*secondary volumes*);
- kopia na dyskach docelowych jest nieodporna na błąd logiczny, dlatego z kopii lustrzanej wykonuje się kopie archiwalne na taśmy. Na czas ich wykonywania kopia lustrzana musi być zamrożona (*split mirror*);
- po zakończeniu kopiowania na taśmy następuje resynchronizacja kopii lustrzanej.

Bardziej zaawansowanym wariantem metody SMB jest struktura trójpoziomowa (por. rys. 6) – zapewnia szybkie odtworzenie w przypadku *rolling disaster* oraz błędu logicznego w danych. W niektórych instalacjach można spotkać strukturę SMB o większej niż trzy liczbie poziomów. W wariancie trójpoziomowym [1], [6]:

- instalowany jest kolejny zestaw dysków (*tertiary*) w ośrodku zapasowym dla kopii błyskawicznych (PiT, ang. *Point in Time*);
- kopia na dyskach *secondary* jest nieodporna na błąd logiczny, dlatego kopia lustrzana musi być zamrożona (*split mirror*) na czas wykonania kopii błyskawicznej na dyski *tertiary*;
- po zakończeniu inicjalizacji kopii błyskawicznej następuje resynchronizacja kopii lustrzanej;
- taśmowa kopia archiwalna wykonywana jest z wolumenów *tertiary*;
- kopia *tertiary* może być używana jako „prawie aktualny" zestaw danych produkcyjnych, który może służyć do operacji typu *read only*, odciążając ośrodek podstawowy.

Kopie błyskawiczne mają na celu uchwycenie spójnego obrazu danych na zadany moment w czasie. Jej koncepcja opiera się na dwóch, podstawowych obserwacjach:

- kopia danych nie jest z reguły potrzebna natychmiast i w całości,
- dane źródłowe nie ulegają zmianom natychmiast i w całości.

Proces wykonywania kopii PiT jest dwufazowy:

- Faza I (inicjalizacji kopii) polega na zestawieniu par źródło-cel.
- Faza II (kopiowania), w zależności od rozwiązania lub wybranej opcji polega na:
  - kopiowaniu w tle całego obrazu źródła,
  - kopiowaniu w tle tylko zaalokowanych fragmentów dysku,
  - kopiowaniu tylko w razie potrzeby (zmiana na wolumenie źródłowym),
  - kopiowaniu przyrostowym od poprzedniego zestawienia.

Po fazie inicjalizacji można już korzystać z logicznie pełnej kopii. Jeżeli odwołanie do kopii „trafia" we fragment nie skopiowany fizycznie, to jest skierowane na źródło. Kopie PiT są zwykle realizowane sprzętowo na poziomie i wewnątrz pojedynczej macierzy.

Zdalne kopie lustrzane, tworzące kopię *secondary* mogą być wykonane jako:

- kopie synchroniczne.
  Realizowane zwykle sprzętowo na poziomie macierzy (rozwiązania programowe są mniej popularne). Zapis na dysk jest uznany za zakończony po stronie ośrodka podstawowego dopiero wtedy, kiedy zostanie potwierdzony zapis po stronie ośrodka zapasowego. Odległość pomiędzy ośrodkami ograniczona jest z ww. powodów technicznych do kilkunastu kilometrów (w praktyce oznacza to odległość do 10 km pomiędzy serwerami i konieczność stosowania wydzielonego łącza o wysokiej przepustowości). Przy intensywnych zapisach na dysk utrzymywanie kopii synchronicznej może mieć negatywny wpływ na wydajność przetwarzania.
- kopie semisynchroniczne.
  Pierwszy zapis po stronie ośrodka podstawowego jest uznany za zakończony bez oczekiwania na potwierdzenie z ośrodka zapasowego, ale kolejne zapisy muszą czekać na potwierdzenie.
- kopie asynchroniczne.
  Wspomagane sprzętowo na poziomie macierzy, realizowane programowo na wydzielonym serwerze (partycji, ang. *System Data Mover*). Zapisy na dyski *secondary* grupowane są w „paczki" (ang. *Consistency Groups*) według znacznika czasu (ang. *Time Stamp*). Spójność tych zapisów jest wspomagana dziennikami zmian utrzymywanymi na serwerze SDM. Rozwiązanie to jest odporne na zagrożenia typu *rolling disaster.* Dane na dyskach *secondary* są opóźnione, w stosunku do danych w ośrodku podstawowym, od kilku

sekund do kilku minut (w praktyce opóźnienia takie występują tylko w godzinach największego wykorzystania systemu, kiedy ilość przesyłanych danych przekracza przepustowość łącza). Dystans pomiędzy ośrodkami nie jest ograniczony. Wykonywanie kopii asynchronicznej ma minimalny wpływ na produkcję.

4. Podsumowanie

W tabeli 4.1 zawarte jest podsumowanie związków pomiędzy formalnymi architekturami zabezpieczania danych a typami ośrodków zapasowych. W niniejszym opracowaniu nie była rozważana strona ekonomiczna przedsięwzięcia budowy i utrzymania ośrodka zapasowego. Nie były także rozważane zalety i wady, zarówno w kontekście technicznym jak i ekonomicznym, różnych rozwiązań organizacyjnych, takich jak kolokacja, hosting, wirtualizacja serwerów czy tzw. przetwarzanie w chmurze (ang. *cloud computing*).

ROI (ang. *return on investment* – zwrot z inwestycji) określa tylko bezpośredni wymiar finansowy inwestycji – nie bierze się pod uwagę skutków pośrednich katastrofy: kosztów odtworzenia, utraty zysków, straty reputacji, itp. Zaawansowane rozwiązania, takie jak zdalne kopie lustrzane i kopie PiT, są realizowane zwykle jako dodatkowo płatna funkcja macierzy dyskowej. Zwykle też narzucone są przez producenta określone wymagania na typ i rodzaj połączenia zdalnego między macierzami. Koszt finansowy oraz organizacyjny (wyszkolenie personelu, wdrożenie i przestrzeganie procedur) takiego rozwiązania jest wysoki. Każda firma lub organizacja, której byt rynkowy zależy od możliwości ciągłego przetwarzania danych, musi przeprowadzić analizę, która wskaże, czy warto inwestować w takie rozwiązanie, czy też wystarczą ośrodki zapasowe typu zimnego lub ciepłego plus odpowiednie, zawczasu przygotowane środki (rezerwa finansowa, ubezpieczenia, umowy z dostawcami) które, uruchomione po katastrofie, pozwolą odtworzyć przetwarzanie bez narażania organizacji na znaczne straty.

Przedstawione w zarysie w rozdz. 2 rozwiązania replikacji danych leżą na ścieżce rozwojowej prowadzącej do intensywnie ostatnio badanych możliwości tzw. *continuous data protection* (CDP), nazywanych też *continuous backup* lub *real-time backup* [15].

Tab. 6. Związki pomiędzy architekturą zabezpieczania danych a typem ośrodka zapasowego

Poziom wg SHARE	Nazwa architektury	Typ ośrodka zapasowego	Sposób wykonywania kopii zapasowej
0	No off-site data	-	Taśmy/dyski
1	Pickup Truck Method (PTAM)	zimny lub wcale[10]	taśmy
2	PTAM+hot site	ciepły, gorący	taśmy
3	Electronic vaulting	gorący	dyski
4	Active secondary site	gorący, lustrzany	replikacja
5	Two-site two-phase commit	gorący, lustrzany,	replikacja
6	Zero data loss	lustrzany	replikacja
7	Automatic site switch	lustrzany	replikacja

Literatura:

[1] AZAGURY A., FACTOR M. E., SATRAN J., *Point-in-Time Copy: Yesterday, Today and Tomorrow*, Massive Storage Systems and Technologies Conference, pp. 259-270, IEEE, 2002.

[2] HUSSONG W.A. Jr., *Ach, więc jesteś nowym BCP managerem?,* Disaster Recovery Journal, http://www.drj.com.

[3] JAKUBOWSKI R., *Od zapasu głowa nie boli*, Computerworld, Nr 10, 2004.

[4] LIDERMAN K. (red), *Bezpieczeństwo teleinformatyczne*, Problemy formalne i techniczne, WAT, Warszawa, 2006.

[5] LIDERMAN K., *Analiza ryzyka i ochrona informacji w systemach komputerowych,* PWN, Warszawa, 2008.

[6] ŁAGOWSKI J., *Disaster: Backup&Recovery – wykonanie kopii DR*, W: materiały IX Konferencji PLOUG, Str. 228-238, Kościelisko, Październik 2003.

[7] ŁAGOWSKI J., *Poziomy rozwiązania „Disaster Recovery"*, W: materiały X Konferencji PLOUG, Str. 141-154, Kościelisko, Październik 2004.

[8] PN-ISO/IEC-17799:2005: *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*.

[9] PN-ISO/IEC 27001:2007: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*.

[10] Miejscem przechowywania kopii zapasowych może być np. skrytka bankowa.

[10] BS 25999-1: 2006: *Business continuity management. Code of practice*.

[11] BS 25999-2: 2007: *Specification for business continuity management*.

[12] Taneja Group, *Combining Storage Capacity Optimization and Replication to Optimize Disaster Recovery Capabilities*, January 2009.

[13] NERC BACKUP CONTROL CENTER, A Reference Document EPRI Project RP2473-68, W: NERC Operating Manual, March 2008.

[14] NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.

[15] Storage Networking Industry Association, http://www.snia.org.

[16] www.gartner.com.

Characteristics of basic types of alternate sites

ABSTRACT: This paper presents basic types of alternate sites (especially dedicated to data replication) and their characteristics. Basic methods of increasing computer systems and data immunity against disaster consequences are also described.

KEY WORDS: disaster recovery, alternate site, continuity, data replication, RTO, RPO, RTA, NRO

Praca wpłynęła do redakcji: 05.05.2009.