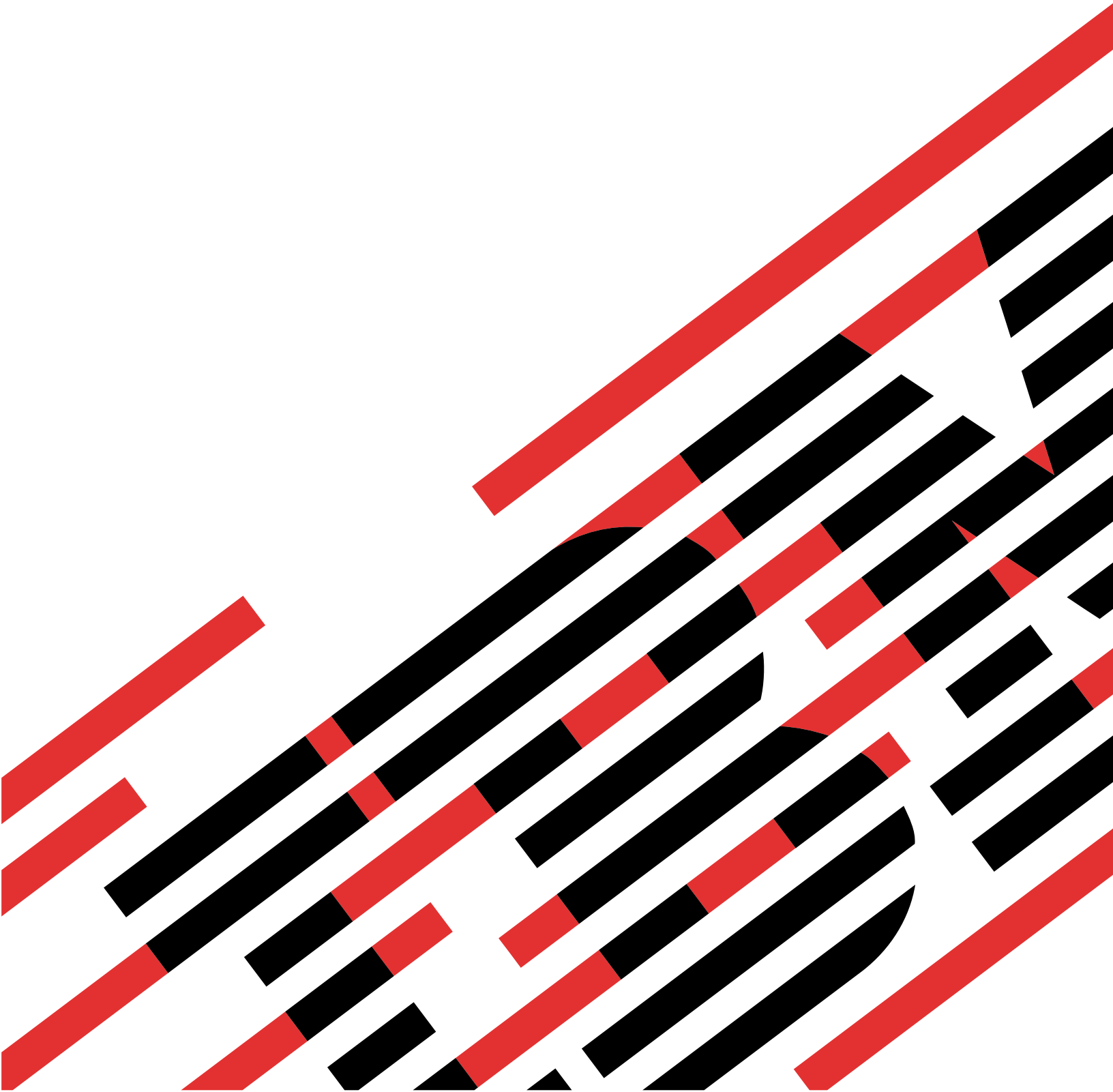
IBM

eserver

iSeries

# Zabezpieczenie dysków



IBM

@server

iSeries

# Zabezpieczenie dysków

# Spis treści

# Część 1. Zabezpieczenie dysków

Oprócz sprawdzonej strategii składowania i odzyskiwania, w systemie powinna funkcjonować również jedna z metod zabezpieczenia danych. Do takich metod należy zabezpieczenie dysków. Zabezpieczenie dysków pomaga chronić dane przed utratą i chroni przed zatrzymaniem systemu w przypadku awarii dysku. Istnieje kilka sposobów zabezpieczenia danych używanych w różnych kombinacjach.

Do pomocy podczas konfigurowania pul dyskowych i zabezpieczania ich przez kontrolę parzystości lub przez zapis lustrzany można użyć kreatorów zarządzania dyskami w iSeries Navigator.

**Uwaga:** Zabezpieczenie dysków skraca czas wyłączenia systemu i przyspiesza odzyskiwanie po awarii, **nie zastępuje** jednak regularnego składowania. W razie całkowitej utraty systemu, awarii procesora albo błędnego działania programu zabezpieczenie dysków nie rozwiązuje problemu.

Poniższe sekcje zawierają informacje dotyczące różnych typów zabezpieczenia dysków i łącznego używania różnych typów zabezpieczenia:

- Wybór narzędzi zabezpieczenia dysków
- Wybór poziomu zabezpieczenia

Przed podjęciem kolejnych kroków warto przejrzeć poniższe sekcje:

- Jak system zarządza pamięcią dyskową
- Jak konfiguruje się dyski

# Rozdział 1. Wybór narzędzi zabezpieczenia dysków

Rozważając sposoby zabezpieczenia przed utratą danych, należy zastanowić się nad następującymi problemami:

**Odzyskiwanie**
Czy można odzyskać utracone informacje przez ich odtworzenie z nośników składowania albo utworzenie ich na nowo?

**Dostępność**
Czy można zmniejszyć albo wyeliminować okres, przez który system jest niedostępny po wystąpieniu problemu?

**Serwis**
Czy można zapewnić obsługę serwisową bez wpływu na dane użytkowników?

Pierwszą linię obrony przed utratą danych stanowi strategia składowania i odzyskiwania. Dlatego należy stworzyć plan regularnego składowania informacji przechowywanych w systemie.

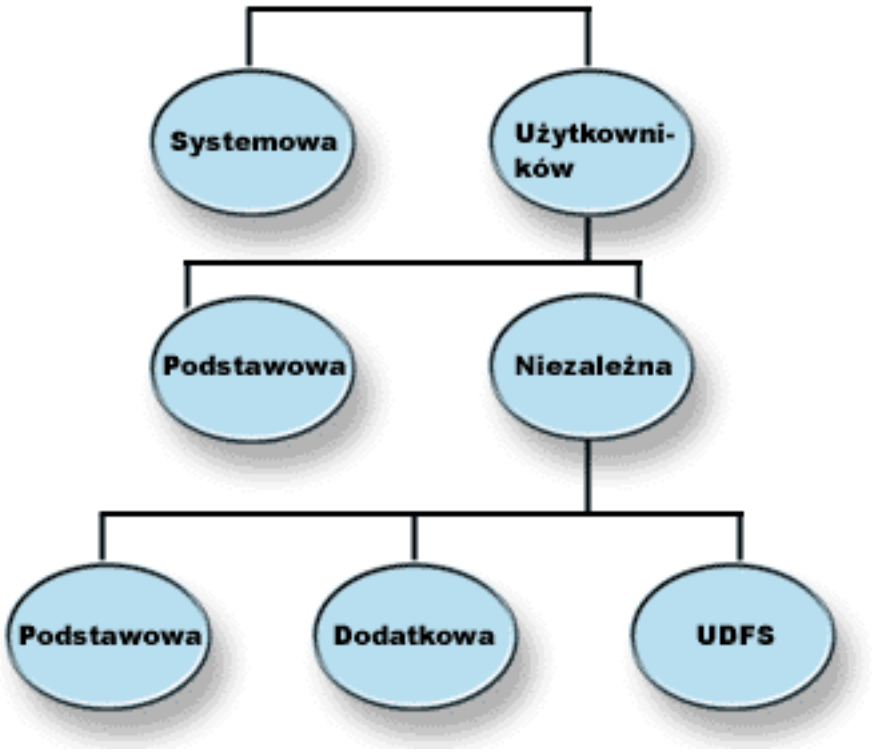
Istnieje wiele narzędzi związanych z dostępnością dysków. Dzięki nim można skrócić albo wyeliminować okresy przestoju systemu i pomóc przy odzyskiwaniu po uszkodzeniu dysku. Informacje na ten temat zawierają następujące sekcje:

- Pule dyskowe
- Sprzętowe zabezpieczenie przez kontrolę parzystości
- Zabezpieczenie przez zapis lustrzany

## Pule dyskowe

Pula dyskowa, zwana również pulą pamięci dyskowej (ASP) w interfejsie znakowym, jest definicją oprogramowania grupy jednostek dyskowych w systemie. Oznacza to, że pula dyskowa niekoniecznie odpowiada fizycznemu rozmieszczeniu dysków. Każda pula dyskowa w systemie jest osobną pulą jednostek dyskowych dla jednego poziomu pamięci. System umieszcza dane we wszystkich jednostkach dyskowych w puli dyskowej. Jeśli wystąpi awaria dysku, należy odtworzyć tylko dane w puli dyskowej, która zawierała uszkodzoną jednostkę. Istnieją dwie podstawowe kategorie pul dyskowych, systemowa pula dyskowa i pule dyskowe użytkowników. Wyróżnia się dwa typy pul dyskowych użytkowników: podstawową i niezależną. Niezależne pule dyskowe dzieli się z kolei na pule dyskowe podstawowe, dodatkowe i UDFS. Poniższe odsyłacze i ilustracja puli dyskowej pomogą zrozumieć zasady działania różnych typów pul dyskowych użytkowników:

- Systemowa pula dyskowa
- Pule dyskowe użytkowników




Pule dyskowe w systemie mogą się składać z wielu jednostek dyskowych. Dla systemu wyglądają one jak pojedyncze jednostki pamięci. System umieszcza dane na wszystkich jednostkach dyskowych. Pul dyskowych można użyć do podzielenia jednostek dyskowych na logiczne podzbiory. Więcej informacji na temat używania pul dyskowych w systemie zawiera sekcja Pule dyskowe — przykłady użycia.

Jeśli jednostki dyskowe zostały przypisane do kilku pul dyskowych, każda pula dyskowa może mieć różne strategie dostępności, składowania i odtwarzania oraz wydajności.

Pule dyskowe ułatwiają odzyskiwanie, jeśli w systemie nastąpi awaria jednostki dyskowej, na skutek której wszystkie dane zostaną utracone. Jeśli taka sytuacja wydarzy się, wymaga się odzyskiwania tylko dla obiektów w puli dyskowej zawierającej uszkodzoną jednostkę dyskową. Obiekty systemowe i obiekty użytkowników w innych pulach dyskowych są zabezpieczone na wypadek awarii dysku. Istnieją również dodatkowe korzyści, ale także pewne koszty i ograniczenia związane z używaniem pul dyskowych.

Więcej informacji na temat pul dyskowych użytkowników zawierają następujące tematy:

- Określanie sposobu konfigurowania pul dyskowych użytkowników
- Uwagi na temat tworzenia nowej puli dyskowej w aktywnym systemie
- Sprawdzenie, czy system ma wystarczającą wielkość obszaru roboczego
- Zróżnicowanie podstawowych i niezależnych pul dyskowych

Więcej informacji na temat implementowania pul dyskowych zawiera podręcznik Składowanie i odtwarzanie.

## Określanie sposobu konfigurowania pul dyskowych użytkowników

Pule dyskowe można wykorzystać, w zależności od potrzeb, mając na uwadze różne cele. Przed skonfigurowaniem pul dyskowych użytkowników należy przejrzeć następujące tematy, które opisują różne sposoby ich używania.

- Używanie pul dyskowych w celu zwiększenia dostępności

- Używanie pul dyskowych w celu zwiększenia wydajności
- Używanie pul dyskowych z obiektami biblioteki dokumentów
- Używanie pul dyskowych z ekstensywnym kronikowaniem
- Używanie pul dyskowych z kronikowaniem ścieżek dostępu

## Używanie pul dyskowych w celu zwiększenia dostępności

Poszczególne części systemu mogą mieć różne wymagania dotyczące dostępności i odzyskiwania. Może istnieć, na przykład, obszerny zbiór historii, zmieniany jedynie na końcu każdego miesiąca. Informacje zawarte w tym zbiorze są użyteczne, lecz mają mniejsze znaczenie. Zbiór ten może zostać umieszczony w osobnej bibliotece w puli dyskowej użytkowników, która nie ma żadnego zabezpieczenia (zabezpieczenie przez zapis lustrzany lub sprzętowe zabezpieczenie przez kontrolę parzystości). Podczas codziennych operacji składowania należy omijać tę bibliotekę. Wymaga ona składowania jedynie gdy jest aktualizowana, tzn. pod koniec miesiąca.

Dokumenty i foldery stanowią inny przykład. Niektóre z nich mają strategiczne znaczenie dla przedsiębiorstwa. Powinno się je chronić za pomocą sprzętowego zabezpieczenia przez kontrolę parzystości lub przez zapis lustrzany, albo też umieścić w zabezpieczonej puli dyskowej użytkowników. Istnieją też dokumenty i foldery przechowywane w systemie w celu dostarczania informacji, lecz rzadko się je zmienia. Mogą się one znajdować w innej puli dyskowej użytkowników o odmiennej strategii składowania i zabezpieczania.

## Używanie pul dyskowych w celu zwiększenia wydajności

Jeśli pule dyskowe użytkowników są używane w celu zwiększenia wydajności systemu, należy wziąć pod uwagę umieszczenie w puli dyskowej jednego obiektu, który jest najbardziej aktywny. W tym przypadku można konfigurować pulę dyskową tylko z jedną jednostką dyskową.

Jednakże przydzielenie puli dyskowej użytkowników jednej jednostki ze sprzętowym zabezpieczeniem przez kontrolę parzystości przeważnie nie powoduje zwiększenia wydajności, ponieważ na wydajność tej jednostki mają wpływ inne jednostki dyskowe w zestawie z kontrolą parzystości.

Przydzielanie jednej puli dyskowej użytkowników specjalnie dziennikom podłączonym do tej samej kroniki może zwiększyć wydajność kronikowania. Jeśli kronika i kronikowane obiekty znajdują się w innej puli dyskowej niż podłączone dzienniki, nie dochodzi do rywalizacji podczas operacji zapisu do dziennika. Położenie jednostek powiązanych z pulą dyskową nie musi być zmieniane przed każdą operacją odczytu lub zapisu.

Aby poprawić wydajność, system rozdziela dzienniki między wiele jednostek dyskowych. Dziennik można umieścić w maksymalnie dziesięciu jednostkach dyskowych w puli dyskowej. Jeśli podana zostanie opcja kronikowania RCVSIZOPT(*MAXOPT1) lub (*MAXOPT2), system może umieścić dziennik w maksymalnie 100 jednostkach dyskowych w puli dyskowej. Jeśli podczas aktywności systemu do puli dyskowej dodanych zostanie więcej jednostek dyskowych, system określi, czy dla dziennika użyć nowych jednostek dyskowych podczas następnego wykonywania funkcji zmiany kroniki.

Innym sposobem zwiększenia wydajności jest zapewnienie wystarczającej liczby jednostek pamięci do obsługi fizycznych operacji wejścia/wyjścia, które są wykonywane na obiektach w puli dyskowej użytkowników. Być może trzeba będzie eksperymentować przenosząc obiekty między pulami dyskowymi, aby sprawdzić, czy jednostki pamięci nie są przeciążone. Więcej informacji na temat pracy ze statusem dysku (komenda WRKDSKSTS) w celu określenia, czy jednostki pamięci nie są przeciążone, zawiera książka *Zarządzanie pracą*  . Jeśli jednostki są przeciążone, należy wziąć pod uwagę dodanie większej ilości jednostek dyskowych do puli dyskowej użytkowników.

## Używanie pul dyskowych z obiektami biblioteki dokumentów

Obiekty biblioteki dokumentów można umieszczać w pulach dyskowych użytkowników. Poniżej przedstawiono zalety umieszczania obiektów DLO w pulach dyskowych użytkowników:

- Możliwość zredukowania czasów składowania dla obiektów DLO i podzielenia ich według wymagań dotyczących składowania.
- Możliwość podzielenia obiektów DLO według ich wymagań dotyczących dostępności. Krytyczne obiekty DLO można umieszczać w pulach dyskowych użytkowników z zabezpieczeniem przez zapis lustrzany lub sprzętowe zabezpieczenie przez kontrolę parzystości. Obiekty DLO, które rzadko się zmieniają, można umieszczać w niechronionych pulach dyskowych z wolniejszymi napędami.
- Możliwość wzrostu liczby dokumentów.

Jeśli w systemie jest zainstalowana bieżąca wersja programu licencjonowanego OS/400, można uruchomić kilka procedur SAVDLO lub RSTDLO dla kilku różnych pul dyskowych. Można również uruchomić kilka operacji SAVDLO w tej samej puli dyskowej.

Jednym ze sposobów rozmieszczania obiektów DLO w pulach dyskowych użytkowników jest pozostawienie w systemowej puli dyskowej tylko systemowych obiektów DLO (foldery dostarczone przez IBM). Inne foldery należy przenieść do pul dyskowych użytkowników. Foldery systemowe rzadko się zmieniają, więc są rzadko składowane. Sekcja ″Jak przenosić foldery do innej puli dyskowej″ w książce Składowanie i odtwarzanie

lub pomiędzy pulami dyskowymi użytkowników opisuje procedurę przenoszenia folderów z systemowej puli dyskowej do pul dyskowych użytkowników.

Pula dyskowa może być parametrem komendy SAVDLO. Umożliwia to zeskładowanie wszystkich obiektów DLO z danej puli dyskowej w określonym dniu tygodnia. Obiekty DLO z puli dyskowej 2 można na przykład składować w poniedziałek, obiekty DLO z puli dyskowej 3 we wtorek i tak dalej. Wszystkie zmienione DLO można też składować codziennie.

Procedura odzyskiwania, jeśli korzysta się z tego sposobu składowania, będzie zależeć od typu utraconych informacji. Jeśli utracie uległa cała pula dyskowa, można odtworzyć ostatnią pełną zeskładowaną kopię obiektów DLO z tej puli dyskowej, a następnie zmienione DLO pochodzące z codziennego składowania.

Jeśli w tej samej operacji składowane są obiekty DLO z więcej niż jednej puli dyskowej, na taśmie zostanie utworzony inny zbiór i numer kolejny dla każdej puli dyskowej. Podczas odtwarzania należy podać odpowiedni numer kolejny. Upraszcza to odtwarzanie zmienionych obiektów DLO do utraconej puli dyskowej bez potrzeby znajomości wszystkich nazw folderów.

Jeśli w komendzie SAVDLO pojawi się wartość DLO(*SEARCH) lub DLO(*CHG), należy, jeśli jest to możliwe, podać pulę dyskową. Podanie puli dyskowej umożliwia składowanie zasobów systemu.

***Ograniczenia dla obiektów DLO w pulach dyskowych użytkowników:*** Ograniczenia te mają zastosowanie podczas umieszczania obiektów DLO w pulach dyskowych użytkowników:

- Jeśli w operacji składowania używany jest zbiór składowania, można składować obiekty DLO tylko z jednej puli dyskowej.
- Jeśli składowanie odbywa się do zbioru składowania i podano SAVDLO DLO(*SEARCH) lub SAVDLO DLO(*CHG), należy podać również pulę dyskową, nawet jeśli wiadomo, że składowane obiekty znajdują się w jednej puli dyskowej.
- Dokumenty, których nie ma w folderach, powinny znaleźć się w tej samej puli dyskowej.
- Pocztę można umieścić w folderze w puli dyskowej użytkowników. Niewypełnioną pocztę przechowuje się w systemowej puli dyskowej.

## Używanie pul dyskowych z ekstensywnym kronikowaniem

Jeśli kroniki i kronikowane obiekty znajdują się w tej samej puli dyskowej co dzienniki, a pula dyskowa jest przepełniona, należy zakończyć kronikowanie wszystkich obiektów i usunąć przepełnienie dla puli dyskowej.

Książka Składowanie i odtwarzanie  opisuje sposób odzyskiwania przepełnionej puli dyskowej.

Jeśli dziennik znajduje się w innej puli dyskowej niż kronika, a pula dyskowa użytkowników, w której znajduje się dziennik, jest przepełniona, należy:

1. Utworzyć nowy dziennik w innej puli dyskowej użytkowników.
2. Zmienić kronikę (komenda CHGJRN), aby podłączyć nowo utworzony dziennik.
3. Zeskładować odłączony dziennik.
4. Usunąć go.
5. Usunąć zawartość przepełnionej puli dyskowej bez zakończenia kronikowania.
6. Utworzyć nowy dziennik w wyczyszczonej puli dyskowej.
7. Dołączyć nowy dziennik za pomocą komendy CHGJRN.

**Uwaga:** Książka Składowanie i odtwarzanie  zawiera więcej informacji o pracy z dziennikami w przypadku przepełnienia puli dyskowej.

### Używanie pul dyskowych z kronikowaniem ścieżek dostępu

Jeśli planuje się użycie kronikowania jawnej ścieżki dostępu, IBM zaleca, aby najpierw na kilka dni zmienić kronikę na dziennik w systemowej puli dyskowej (pula dyskowa 1). Przed przydzieleniem konkretnej wielkości dla puli dyskowej użytkowników należy uruchomić kronikowanie ścieżek dostępu, aby sprawdzić, czy spełnione zostały wymagania dotyczące pamięci dla dziennika. Zarządzanie kronikami udostępnia więcej informacji dotyczących sposobu określania wymagań związanych z pamięcią przeznaczoną do kronikowania.

## Uwagi na temat tworzenia nowej puli dyskowej w aktywnym systemie

Począwszy od wersji V3R6 programu licencjonowanego OS/400, można dodawać jednostki dyskowe do puli ASP w aktywnym systemie. Podczas dodawania jednostek dyskowych do puli dyskowej, która nie istnieje, system tworzy nową pulę dyskową. Sekcja Dodawanie jednostki dyskowej lub puli dyskowej zawiera kroki konfigurowania puli dyskowej. Jeśli nowa pula dyskowa użytkowników zostanie utworzona w aktywnym systemie, należy sprawdzić, czy zrozumiane zostały następujące uwagi:

- Nie można uruchamiać zabezpieczenia przez zapis lustrzany dla podstawowej puli dyskowej, gdy system jest aktywny. W aktywnym systemie zabezpieczenie przez zapis lustrzany można uruchomić tylko dla niedostępnej niezależnej puli dyskowej. Nowa pula dyskowa nie jest w pełni zabezpieczona, chyba że wszystkie pule dyskowe mają sprzętowe zabezpieczenie przez kontrolę parzystości.
- Nie można przenosić istniejących jednostek dyskowych do podstawowych pul dyskowych, gdy system jest aktywny. Wraz z jednostką dyskową przenoszone są dane. Można to zrobić wyłącznie za pomocą Dedykowanych narzędzi serwisowych (Dedicated Service Tools - DST). Nie jest możliwe przeniesienie jednostek dyskowych z istniejącej puli dyskowej do niezależnej puli dyskowej.
- System używa wielkości puli dyskowej użytkowników do określenia wartości progowej pamięci dla dzienników używanych przez system-managed access-path protection (SMAPP). Jeśli pula dyskowa została utworzona w aktywnym systemie, funkcja SMAPP przyjmuje, że jej wielkość jest równa wielkości przypisanych do niej jednostek dyskowych. Na przykład przyjmijmy, że dodawane są 2 jednostki dyskowe do nowej puli dyskowej o numerze 2. Łączna pojemność 2 jednostek dyskowych wynosi 2062 MB. Później dodano jeszcze dwie jednostki, aby zwiększyć pojemność do 4124 MB. Dla funkcji SMAPP, wielkością puli dyskowej pozostaje 2062 MB do momentu następnego wykonania IPL lub udostępnienia niezależnej puli dyskowej. Oznacza to, że próg pamięci dzienników SMAPP jest niższy i system musi częściej zmieniać te pliki. Zwykle nie ma to większego wpływu na wydajność systemu.

System określa pojemność każdej puli dyskowej podczas wykonywania IPL lub udostępnienia niezależnej puli dyskowej. Obliczana wówczas jest wymagana wielkość SMAPP. Sekcja Funkcja SMAPP (System-managed access-path protection) zawiera więcej informacji na temat funkcji SMAPP.

## Sprawdzenie, czy system ma wystarczającą wielkość obszaru roboczego

Podczas wprowadzania zmian w konfiguracji dysków system może potrzebować obszaru roboczego. Na przykład wtedy, gdy planowane jest przeniesienie jednostek dyskowych z jednej puli dyskowej do innej puli dyskowej. Zanim zostaną one przeniesione, system musi przenieść wszystkie dane do innej jednostki dyskowej. Sekcja ″Sposób określania wymagań dla puli pamięci dyskowej″ w książce Składowanie i odtwarzanie  zawiera przykłady określania wielkości obszaru roboczego potrzebnego w danej sytuacji. Opisuje również systemowe ograniczenia wielkości pamięci dyskowej.

Jeśli system nie posiada wystarczającej ilości pamięci dla zaspokojenia chwilowych potrzeb, można zacząć od wyczyszczenia pamięci dyskowej. Wielokrotnie zdarza się, że użytkownicy przetrzymują w systemie zbędne obiekty, takie jak stare kolejki wydruków lub dokumenty. W takiej sytuacji przydatna okazuje się funkcja automatycznego czyszczenia dostępna z Asysty Operacyjnej - pozwala ona zwolnić pewną ilość pamięci w systemie.

Jeśli wyczyszczenie zbędnych obiektów w pamięci dyskowej nadal nie zapewnia wystarczającej tymczasowej przestrzeni dyskowej, inne rozwiązanie stanowi czasowe usunięcie obiektów z systemu. Na przykład, jeśli planowane jest przeniesienie dużej biblioteki do nowej puli dyskowej użytkowników, można zeskładować bibliotekę i usunąć ją z systemu. Następnie, po przeniesieniu jednostek dyskowych, należy odtworzyć tę bibliotekę. Oto przykład:

1. Zeskładuj prywatne uprawnienia do obiektów w systemie, pisząc:
   `SAVSECDTA DEV(napęd_taśm)`
2. Zeskładuj obiekt, używając odpowiedniej komendy SAVxxx. Na przykład, aby zeskładować bibliotekę, użyj komendy SAVLIB. Rozważ dwukrotne składowanie obiektów na dwóch różnych taśmach.
3. Usuń obiekt z systemu, używając odpowiedniej komendy DLTxxx. Na przykład, aby usunąć bibliotekę, użyj komendy DLTLIB.
4. Ponownie oblicz pojemność dysku, aby określić czy zwolniłeś wystarczającą ilość pamięci dla zaspokojenia chwilowych potrzeb.
5. Jeśli została zwolniona wystarczająca ilość pamięci, skonfiguruj dyski.
6. Odtwórz usunięte obiekty.

### Pule dyskowe — przykłady użycia

Pule dyskowe są używane do spełniania wymagań dotyczących wydajności systemu i składowania:

- Pulę dyskową tworzy się, aby zapewnić dedykowane zasoby dla często używanych obiektów, takich jak dzienniki.
- Pulę dyskową tworzy się dla zbiorów składowania. Obiekty można składować do zbiorów składowania w innej puli dyskowej. Mało prawdopodobna jest utrata puli dyskowej zawierającej obiekt i jednocześnie puli dyskowej zawierającej zbiór składowania.
- Osobne pule dyskowe tworzy się dla obiektów z różnymi wymaganiami dotyczącymi odzyskiwania i ich dostępności. Na przykład można umieścić krytyczne zbiory bazy danych lub dokumenty w puli dyskowej z zabezpieczeniem przez zapis lustrzany lub sprzętowym zabezpieczeniem przez kontrolę parzystości.
- Pulę dyskową tworzy się dla rzadko używanych obiektów, takich jak duże zbiory historii w jednostkach dyskowych o mniejszej wydajności.
- Pul dyskowych można użyć do zarządzania czasami odzyskiwania ścieżek dostępu do krytycznych i niekrytycznych zbiorów baz danych korzystających z funkcji SMAPP.
- Niezależna pula dyskowa może być używana do izolowania rzadko wykorzystywanych danych w celu zwolnienia zasobów systemu używanych tylko wtedy, gdy są potrzebne.
- Niezależna pula dyskowa w środowisku z klastrami pozwala udostępniać pamięć dyskową, którą można przełączać, co zapewnia stały dostęp do zasobów.

## Pule dyskowe — zyski

Umieszczanie obiektów w pulach dyskowych użytkowników, zwanych również pulami pamięci dyskowej (ASP) w interfejsie znakowym, ma wiele zalet. Wśród nich należy wymienić:

- **Dodatkowe zabezpieczenie danych.** Oddzielając biblioteki, dokumenty lub inne obiekty w puli dyskowej użytkowników można uniknąć utraty danych w przypadku awarii jednostki dyskowej w systemowej lub innej puli dyskowej. Na przykład, jeśli doszło do awarii jednostki dyskowej i dane w systemowej puli dyskowej zostały utracone, obiekty w pulach dyskowych użytkowników pozostały nietknięte i można je wykorzystać do odzyskiwania obiektów w systemowej puli dyskowej. Jeśli awaria powoduje utratę danych z puli dyskowej użytkowników, dane w systemowej puli dyskowej pozostają nietknięte.
- **Zwiększenie wydajności systemu.** Używanie pul dyskowych pozwala również zwiększyć wydajność systemu. Jest to spowodowane tym, że system dedykuje jednostki dyskowe powiązane z pulą dyskową obiektom w tej puli dyskowej. Załóżmy, że w systemie intensywnie wykorzystuje się kronikowanie. Umieszczenie kronik i kronikowanych obiektów oraz dzienników w dwóch różnych pulach dyskowych zmniejsza rywalizację pomiędzy nimi o dostęp do zasobów, co zwiększa wydajność kronikowania. Aby zmniejszyć rywalizację, można użyć niezależnych pul dyskowych, umieszczając obiekty, które mają być kronikowane, w podstawowej puli dyskowej, a dzienniki w jednej lub kilku dodatkowych pulach dyskowych.

  Umieszczanie wielu aktywnych dzienników w tej samej puli dyskowej nie jest najlepszym rozwiązaniem. W wyniku rywalizacji pomiędzy nimi o dostęp do operacji zapisu w puli dyskowej może zmniejszyć się wydajność systemu. Aby uzyskać maksymalną wydajność, należy umieścić każdy aktywny dziennik w oddzielnej puli dyskowej użytkowników.
- **Rozdzielenie obiektów o różnych wymaganiach dotyczących dostępności i odzyskiwania.** Dla różnych pul dyskowych można używać różnych zabezpieczeń. Można również zastosować inne docelowe czasy odzyskiwania ścieżek dostępu dla różnych ASP. Należy też przypisać krytyczne lub częściej używane obiekty do zabezpieczonych jednostek dyskowych o dużej wydajności oraz przypisać duże, mało używane zbiory, takie jak zbiory historii, do niezabezpieczonych jednostek dyskowych o małej wydajności.
- **Większa dostępność i elastyczność**. Sekcja Zalety niezależnych pul dyskowych zawiera opis zalet cechujących niezależne pule dyskowe.

## Pule dyskowe — koszty i ograniczenia

Istnieje kilka specyficznych ograniczeń, z którymi można się zetknąć podczas używania pul dyskowych (pul pamięci dyskowej):

- System nie potrafi bezpośrednio odtworzyć danych utraconych w wyniku awarii nośnika jednostki dyskowej. Sytuacja taka wymaga wykonania operacji odzyskiwania.
- Używanie pul dyskowych może wymagać dodatkowych napędów dysków.
- Używanie pul dyskowych wymaga zarządzania ilością danych w puli dyskowej i unikania jej przepełnienia.
- W przypadku przepełnienia podstawowej puli dyskowej należy podjąć specjalne kroki w celu odzyskiwania.
- Używanie pul dyskowych wymaga zarządzania powiązanymi obiektami. Niektóre pokrewne obiekty, takie jak kroniki i obiekty kronikowane, muszą należeć do tej samej puli dyskowej użytkowników.

## Systemowa pula dyskowa

System automatycznie tworzy systemową pulę dyskową (pulę dyskową 1), która zawiera jednostkę dyskową 1 i wszystkie pozostałe skonfigurowane dyski nieprzypisane do żadnej puli dyskowej użytkowników. Systemowa pula dyskowa zawiera wszystkie obiekty systemowe dla programu licencjonowanego OS/400 i wszystkie obiekty użytkowników, które nie są przypisane do podstawowej lub niezależnej puli dyskowej.

**Uwaga:** W systemie istnieją jednostki dyskowe, które nie zostały skonfigurowane i w związku z tym nie są używane. Są to **nieskonfigurowane** jednostki dyskowe.

Określając pojemność systemowej puli dyskowej i zabezpieczając systemową pulę dyskową należy zwrócić uwagę na następujące zagadnienia.

***Pojemność systemowej puli dyskowej:*** Jeśli systemowa pula dyskowa będzie pełna, system przerwie normalne działanie. Należy wówczas wykonać IPL i podjąć działania naprawcze (takie jak usuwanie obiektów), aby zabezpieczyć się przed ponownym przepełnieniem.

Można także ustalić próg, po przekroczeniu którego operator systemu zostanie powiadomiony o możliwym braku wolnego miejsca. Na przykład, jeśli ustawiono wartość progową dla systemowej puli dyskowej i wynosi ona 80, kolejka komunikatów operatora systemu (QSYSOPR) i kolejka komunikatów systemowych (QSYSMSG) zostaną powiadomione o tym, że systemowa pula dyskowa jest w 80% zapełniona. Komunikat jest wysyłany co godzinę, do momentu zmiany wartości progowej lub usunięcia obiektów czy przesłania ich z systemowej puli dyskowej w inne miejsce. Jeśli komunikat ten zostanie zignorowany, systemowa pula dyskowa całkowicie zapełni się i praca systemu zostanie w nienormalny sposób przerwana.

Istnieje także trzecia metoda zabezpieczania systemowej puli dyskowej przed przeładowaniem wykorzystująca wartości systemowe QSTGLOWLMT i QSTGLOWACN. Więcej informacji na ten temat zawiera sekcja ″Jak zmienić wartość progową dla systemowej puli pamięci dyskowej″ w książce

Składowanie i odtwarzanie  .

***Zabezpieczanie systemowej puli dyskowej:*** IBM zaleca, aby używać zabezpieczenia przez sprzętową kontrolę parzystości lub zabezpieczenia przez zapis lustrzany w systemowej puli dyskowej. Używanie narzędzi zabezpieczania dysków zmniejsza ryzyko utraty danych z systemowej puli dyskowej. Jeśli dostęp do systemowej puli dyskowej zostanie utracony, adresowalność obiektów w każdej puli dyskowej użytkowników również zostanie utracona.

Utraconą możliwość dostępu można odzyskać przez odtworzenie całego systemu lub przez użycie komendy Odzyskiwanie pamięci (Reclaim Storage - RCLSTG). Komenda RCLSTG nie jest jednak w stanie odtworzyć informacji o właścicielach obiektów. Po jej zastosowaniu właścicielem wszystkich obiektów będzie profil użytkownika QDFTOWN. Do odtworzenia informacji o właścicielach obiektów biblioteki dokumentów można użyć komendy Odzyskanie obiektu biblioteki dokumentów (Reclaim Document Library Object - RCLDLO).

## Pule dyskowe użytkowników

Pulę dyskową użytkowników można utworzyć poprzez zgrupowanie zestawu jednostek dyskowych i przypisanie tej grupy do puli dyskowej. Pule dyskowe użytkowników mogą zawierać biblioteki, dokumenty i obiekty innych typów. Pule dyskowe użytkowników istnieją w dwóch formach: podstawowe pule dyskowe i niezależne pule dyskowe. W środowisku z klastrami niezależne pule dyskowe można przełączać pomiędzy systemami bez konieczności wykonywania IPL, co umożliwia stałą dostępność danych. Podstawowe pule dyskowe mają numery od 2 do 32. Niezależne pule dyskowe mają numery od 33 do 255. Aby uzyskać więcej informacji na temat różnic pomiędzy niezależnymi i podstawowymi pulami dyskowymi, należy przejrzeć sekcję Różnice pomiędzy podstawową i niezależną pulą dyskową.

Poniższe tematy zawierają więcej informacji o bibliotecznych i niebibliotecznych pulach dyskowych:

- Biblioteczne pule dyskowe użytkowników
- Niebiblioteczne pule dyskowe użytkowników

Po skonfigurowaniu pul dyskowych należy zabezpieczyć je używając zapisu lustrzanego lub zabezpieczenia przez sprzętową kontrolę parzystości.

***Biblioteczne pule dyskowe użytkowników:*** Biblioteczne pule dyskowe użytkowników zawierają biblioteki i systemy plików zdefiniowane przez użytkownika (UDFS). IBM zaleca, aby używać bibliotecznych pul dyskowych użytkowników, ponieważ kroki odzyskiwania są wtedy prostsze niż w przypadku niebibliotecznych pul dyskowych użytkowników. Istnieje wiele czynników, które należy uwzględnić podczas używania bibliotecznych pul dyskowych użytkowników.

***Co należy wiedzieć o bibliotecznych pulach dyskowych użytkowników:***

- W puli dyskowej użytkowników **nie należy** tworzyć bibliotek systemowych, bibliotek produktów (biblioteki, których nazwy zaczynają się od Q lub #) ani folderów (foldery, których nazwy zaczynają się od Q). W puli dyskowej użytkowników **nie należy** odtwarzać żadnej z tych bibliotek ani folderów. Działanie takie może wywołać nieprzewidziane skutki.
- Biblioteczne pule dyskowe użytkowników mogą zawierać zarówno biblioteki, jak i obiekty biblioteki dokumentów. Biblioteka dokumentów dla puli dyskowej użytkowników ma nazwę QDOCnnnn, gdzie *nnnn* jest numerem puli dyskowej.
- Kroniki i obiekty, które są kronikowane, **muszą** znajdować się w tej samej puli dyskowej. Dziennik należy umieścić w innej puli dyskowej. Zabezpiecza to, w razie wystąpienia awarii dysku, przed jednoczesną utratą obiektów i dzienników.

  Aby zacząć kronikowanie, kronika (obiekt typu *JRN) i obiekt, który ma być kronikowany, muszą znajdować się w tej samej puli dyskowej. W celu rozpoczęcia kronikowania, należy użyć poniższych komend.
  - Uruchomienie kronikowania zbioru fizycznego (Start Journal Physical File - STRJRNPF) - komenda dla zbiorów fizycznych.
  - Uruchomienie kronikowania ścieżek dostępu (Start Journal Access Path - STRJRNAP) - komenda dla ścieżek dostępu.
  - Komenda Uruchomienie kronikowania (Start Journal - STRJRN) dla obiektów zintegrowanego systemu plików.
  - Uruchomienie kronikowania obiektu (Start Journal Object - STRJRNOBJ) - komenda dla innych typów obiektów.

  Kronikowania nie można powtórzyć dla obiektu zeskładowanego, a następnie odtworzonego w innej puli dyskowej, która nie zawiera kroniki. Kronika i obiekt muszą znajdować się w tej samej puli dyskowej, aby ponownie automatycznie uruchamiać kronikowanie dla obiektu.
- Sieć baz danych nie może przekraczać granic puli dyskowej. Nie można utworzyć zbioru w jednej puli dyskowej, a zależnego od niego zbioru logicznego w innej puli dyskowej. Wszystkie podstawowe zbiory fizyczne dla zbioru logicznego muszą znajdować się w tej samej puli dyskowej, co zbiór fizyczny. System tworzy ścieżki dostępu tylko dla zbiorów baz danych znajdujących się w tej samej puli dyskowej, co podstawowy zbiór fizyczny (ograniczenie to nie dotyczy zapytań tymczasowych). Ścieżki dostępu nie są nigdy współużytkowane przez zbiory znajdujące się w różnych pulach dyskowych. Formaty rekordów nie są zaś współużytkowane pomiędzy różnymi pulami dyskowymi. Z tego powodu żądanie formatu zostanie zignorowane i utworzy się nowy format.
- W ASP użytkowników można umieścić kolekcję SQL. Podczas tworzenia kolekcji należy podać docelową pulę dyskową.
- Jeśli biblioteczna pula dyskowa użytkowników nie zawiera żadnych zbiorów baz danych, należy wybrać *NONE jako docelową godzinę odzyskiwania ścieżki dostępu dla puli dyskowej. Taka sytuacja może się zdarzyć na przykład wtedy, gdy biblioteczna pula dyskowa użytkowników zawiera jedynie biblioteki dla dzienników. Jeśli jako godzinę odzyskiwania ścieżki dostępu wybierze się *NONE, uniemożliwi to systemowi wykonanie zbędnych działań dla tej puli dyskowej. Funkcja SMAPP (System-managed access-path protection) określa sposób ustawiania godziny odzyskiwania ścieżki dostępu.

***Niebiblioteczne pule dyskowe użytkowników:*** Niebiblioteczne pule dyskowe użytkowników zawierają kroniki, dzienniki i zbiory składowania, których biblioteki znajdują się w systemowej puli dyskowej.

Jeśli czasy odtwarzania ścieżek dostępu przypisuje się pojedynczym pulom dyskowym, dla niebibliotecznej puli dyskowej użytkowników należy ustawić docelowy czas odtwarzania *NONE. Niebiblioteczna pula dyskowa użytkowników nie może zawierać żadnych zbiorów i z tego powodu nie może korzystać z funkcji SMAPP (system-managed access-path protection). Wybranie czasu odzyskiwania ścieżek dostępu dla niebibliotecznej puli dyskowej użytkowników o wartości innej niż *NONE sprawia, że system wykonuje dodatkową nieprzynoszącą korzyści pracę. Sekcja Funkcja SMAPP opisuje sposób definiowania czasów odtwarzania ścieżek dostępu.

***Zabezpieczanie pul dyskowych:*** Uwagi dotyczące ochrony pul dyskowych:

- Wszystkie pule dyskowe, włącznie z systemową pulą dyskową, powinny mieć zabezpieczenie przez zapis lustrzany lub powinny w całości składać się z jednostek dyskowych ze sprzętowym zabezpieczeniem przez kontrolę parzystości, aby zapewnić nieprzerwane działanie systemu po awarii dysku w puli dysków.
- Jeśli awaria dysku wystąpi w puli dyskowej nieposiadającej zabezpieczenia przez zapis lustrzany, praca systemu może zostać przerwana, co zależy od typu jednostki dyskowej i rodzaju błędu.
- Jeśli awaria dysku wystąpi w puli dyskowej dysponującej zabezpieczeniem przez zapis lustrzany, system będzie nadal działał (chyba że awarii uległy obie lustrzane jednostki pamięci).
- Jeśli jednostka dyskowa ulegnie awarii w puli dyskowej ze sprzętowym zabezpieczeniem przez kontrolę parzystości, system będzie nadal działał do momentu wystąpienia awarii innej jednostki dyskowej w tej samej puli dyskowej.

***Ograniczenia systemowe dla pamięci puli dyskowej:*** Podczas IPL system ustala ilość pamięci dyskowej skonfigurowanej w systemie. Ogólna ilość pamięci stanowi sumę pojemności skonfigurowanych jednostek i ich par lustrzanych, jeśli takie występują. Nie wlicza się nieskonfigurowanych jednostek dyskowych. Ilość pamięci dyskowej porównuje się z jej maksimum obsługiwanym przez dany model.

Jeśli skonfigurowano więcej pamięci dyskowej niż jest to dopuszczalne, do kolejki komunikatów operatora systemu (CPI1158) (QSYSOPR) i do kolejki komunikatów QSYSMSG (o ile istnieje) przesyłany jest komunikat. Komunikat ten wskazuje, że w systemie występuje za dużo pamięci dyskowej. Jest on wysyłany podczas każdego IPL tak długo, jak ilość pamięci dyskowej przekracza dopuszczalne maksimum.

## Niezależne pule dyskowe

Terminy **niezależna pula pamięci dyskowej** i **niezależna pula dyskowa** są synonimami.

Niezależna pula dyskowa jest kolekcją jednostek dyskowych, które mogą być dostępne (online) lub niedostępne (offline) niezależnie od reszty pamięci w systemie, włącznie z systemową pulą dyskową, pulami dyskowymi użytkowników i innymi niezależnymi pulami dyskowymi. Niezależne pule dyskowe są użyteczne zarówno w pojedynczym systemie, jak i w środowiskach składających się z wielu systemów. Aby uzyskać informacje pokrewne, należy zapoznać się z tematami opisującymi systemową pulę dyskową i pulę dyskową użytkowników.

W środowisku z pojedynczym systemem niezależna pula dyskowa może być dostępna w trybie offline niezależnie od innych pul dyskowych, ponieważ dane w niej zawarte nie są podzielone. Znaczy to, że w niezależnej puli dyskowej znajdują się wszystkie niezbędne informacje systemowe powiązane z danymi z tej puli. Niezależna pula dyskowa może być również wprowadzona w tryb online, gdy system jest aktywny (nie jest wymagane IPL). Używanie niezależnych pul dyskowych w ten sposób jest bardzo użyteczne wtedy, gdy istnieje duża ilość danych niepotrzebnych w codziennej pracy. Niezależna pula dyskowa zawierająca te dane może pozostać w trybie offline do momentu, kiedy będzie potrzebna. Ponieważ zwykle większość pamięci jest odłączona, może to skrócić czas przetwarzania dla operacji takich jak IPL czy odzyskiwanie pamięci.

W środowiskach składających się z wielu systemów niezależna pula dyskowa może być przełączana pomiędzy systemami. **Przełączana niezależna pula dyskowa** jest zestawem jednostek dyskowych, które można przełączać pomiędzy systemami, aby każdy system miał dostęp do danych. Dostęp do danych ma w określonym momencie tylko jeden system. Podobnie jak w środowisku z pojedynczym systemem, niezależna pula dyskowa może być przełączana, ponieważ nie jest podzielona. Przełączane niezależne pule dyskowe mogą pomóc w takich operacjach, jak:
- utrzymywanie danych dostępnych dla aplikacji nawet w przypadku wyłączenia pojedynczego systemu (zaplanowanego lub niezaplanowanego),
- wyeliminowanie procesu replikowania danych z jednego systemu do drugiego,
- usunięcie, w niektórych sytuacjach, awarii jednostki dyskowej z niezależnej puli dyskowej,
- osiągnięcie wysokiej dostępności i skalowalności.

Więcej informacji zawiera temat Niezależna pula dyskowa.

### Różnice pomiędzy podstawową i niezależną pulą dyskową

Podstawowe pule dyskowe i niezależne pule dyskowe, nazywane również pulami pamięci dyskowej (ASP) w interfejsie znakowym, są użyteczne podczas grupowania jednostek dyskowych zawierających konkretne informacje; jednakże istnieją pomiędzy nimi różnice:

- Podczas wykonywania IPL serwera wszystkie jednostki dyskowe skonfigurowane dla podstawowej puli dyskowej muszą być zaewidencjonowane tak, aby serwer mógł kontynuować IPL. Niezależne pule dyskowe nie zostaną włączone do IPL. Podczas udostępniania niezależną pulę dyskową, węzeł sprawdza, czy wszystkie jednostki dyskowe są obecne.
- Jeśli niezabezpieczona jednostka dyskowa w puli dyskowej ulegnie awarii, wszystkie normalne operacje na serwerze wstrzymuje się do momentu jej naprawy. Całkowita utrata jednostki dyskowej w podstawowej puli dyskowej wymaga długich procedur odzyskiwania w celu odtworzenia utraconych danych, zanim serwer będzie mógł wykonać IPL i powrócić do normalnej pracy.
- Dane w podstawowej puli dyskowej należą do węzła przypisania i mogą być udostępnione w systemie. W niezależnej puli dyskowej dane nie należą do węzła, ale do niezależnej puli dyskowej. Dane w niezależnej puli dyskowej pomiędzy węzłami w klastrze można współużytkować poprzez zablokowanie ich dla jednego węzła i udostępnienie dla drugiego.
- Podczas tworzenia podstawowej puli dyskowej przypisuje się jej numer. Podczas tworzenia niezależnej puli dyskowej nadaje się jej nazwę, a numer przypisuje system.
- Jeśli podstawowa pula dyskowa jest pełna, może przenieść nadwyżkę danych do systemowej puli dyskowej. Niezależne pule dyskowe nie mogą być przepełnione. Gdyby do tego doszło, oznaczałoby to, że straciły one swoją niezależność. Jeśli zajętość niezależnej puli dyskowej zbliża się do wartości progowej, należy dodać więcej jednostek dyskowych lub usunąć obiekty, aby zwolnić pamięć.
- Po wprowadzaniu zastrzeżonych zmian w konfiguracji dysku należy w podstawowej puli dyskowej zrestartować serwer do narzędzi DST. W przypadku niezależnej puli dyskowej działającej w trybie offline serwer nie musi działać w trybie DST, aby uruchomić lub zatrzymać zabezpieczenie przez sprzętową kontrolę parzystości, uruchomić kompresję, usunąć jednostkę dyskową itd.

## Sprzętowe zabezpieczenie przez kontrolę parzystości

Sprzętowe zabezpieczenie przez kontrolę parzystości jest funkcją sprzętową, która zabezpiecza przed utratą danych w wyniku awarii lub uszkodzenia dysku. Aby zabezpieczyć dane, adapter wejścia/wyjścia (IOA) oblicza i zapisuje wartości parzystości dla każdego bitu danych. IOA oblicza wartość parzystości na podstawie danych w tym samym miejscu w każdej z pozostałych jednostek dyskowych z grupy urządzeń parzystości. W przypadku uszkodzenia dysku dane można zrekonstruować, używając zapisanego bitu parzystości i bitów znajdujących się w tych samych miejscach na każdym z pozostałych dysków. Podczas rekonstrukcji danych system może normalnie pracować. Ogólnym celem sprzętowego zabezpieczenia przez kontrolę parzystości jest zapewnienie wysokiej dostępności i zabezpieczenie danych w sposób najtańszy z możliwych.

Jeśli to możliwe, należy zabezpieczyć wszystkie jednostki dyskowe w systemie, stosując albo sprzętowe zabezpieczenie przez kontrolę parzystości, albo zabezpieczenie przez zapis lustrzany. Uchroni to przed utratą informacji w przypadku wystąpienia awarii dysku. W wielu przypadkach podczas naprawy lub wymiany jednostek dyskowych system może normalnie pracować.

**Uwaga:** Sprzętowe zabezpieczenie przez kontrolę parzystości **nie zastępuje** procedur składowania i odzyskiwania danych. Może jednak uchronić system przed zatrzymaniem, gdy wystąpią pewne typy awarii. W niektórych przypadkach może przyspieszać odzyskiwanie danych. Sprzętowe zabezpieczenie przez kontrolę parzystości nie zabezpiecza jednak przed wieloma typami awarii, takimi jak całkowite zniszczenie sprzętu albo błąd operatora lub programisty. Nie zabezpiecza przed wyłączeniem systemu z użytkowania w wyniku awarii innych urządzeń związanych z dyskami (np. kontrolery, dyskowe procesory wejścia/wyjścia (IOP) czy magistrala systemowa).

Zanim zostanie użyte sprzętowe zabezpieczenie przez kontrolę parzystości, należy dokładnie poznać związane z nim korzyści, ale także koszty i ograniczenia.

Dalsze informacje na temat sprzętowego zabezpieczenia przez kontrolę parzystości znajdują się w następujących sekcjach:
- Planowanie sprzętowego zabezpieczenia przez kontrolę parzystości
- Wpływ sprzętowego zabezpieczenia przez kontrolę parzystości na wydajność
- Łączne użycie sprzętowego zabezpieczenia przez kontrolę parzystości i zabezpieczenia przez zapis lustrzany

Więcej informacji na temat sprzętowego zabezpieczenia przez kontrolę parzystości zawiera książka

Składowanie i odtwarzanie. 

## Planowanie sprzętowego zabezpieczenia przez kontrolę parzystości

Aby utworzyć system zabezpieczony przed utratą danych i dysponujący możliwością naprawy podczas pracy, należy zaplanować używanie obydwu zabezpieczeń: przez zapis lustrzany i sprzętowego zabezpieczenia przez kontrolę parzystości. Dla każdego zestawu sprzętowego zabezpieczenia przez kontrolę parzystości wykorzystywany na informacje o parzystości obszar odpowiada jednej jednostce dyskowej. Począwszy od adapterów wejścia/wyjścia (IOA) w wersji V5R2 minimalna liczba jednostek dyskowych w zestawie parzystości wynosi 3; maksymalna liczba jednostek dyskowych w zestawie parzystości wynosi 18. W przypadku adapterów wejścia/wyjścia (IOA) w wersjach wcześniejszych niż V5R2 minimalna liczba jednostek dyskowych w zestawie parzystości wynosi 4; maksymalna liczba jednostek dyskowych w zestawie parzystości wynosi 10. W wersji V5R2 można optymalizować zestawy parzystości pod kątem pojemności, wydajności lub zrównoważenia obciążenia, jeśli adapter IOA jest w wersji V5R2 lub nowszej. Aby uzyskać więcej informacji na temat implementacji sprzętowego zabezpieczenia przez kontrolę parzystości i sposobu jego wykorzystania w połączeniu z zabezpieczeniem przez zapis lustrzany, należy przejrzeć poniższe tematy.

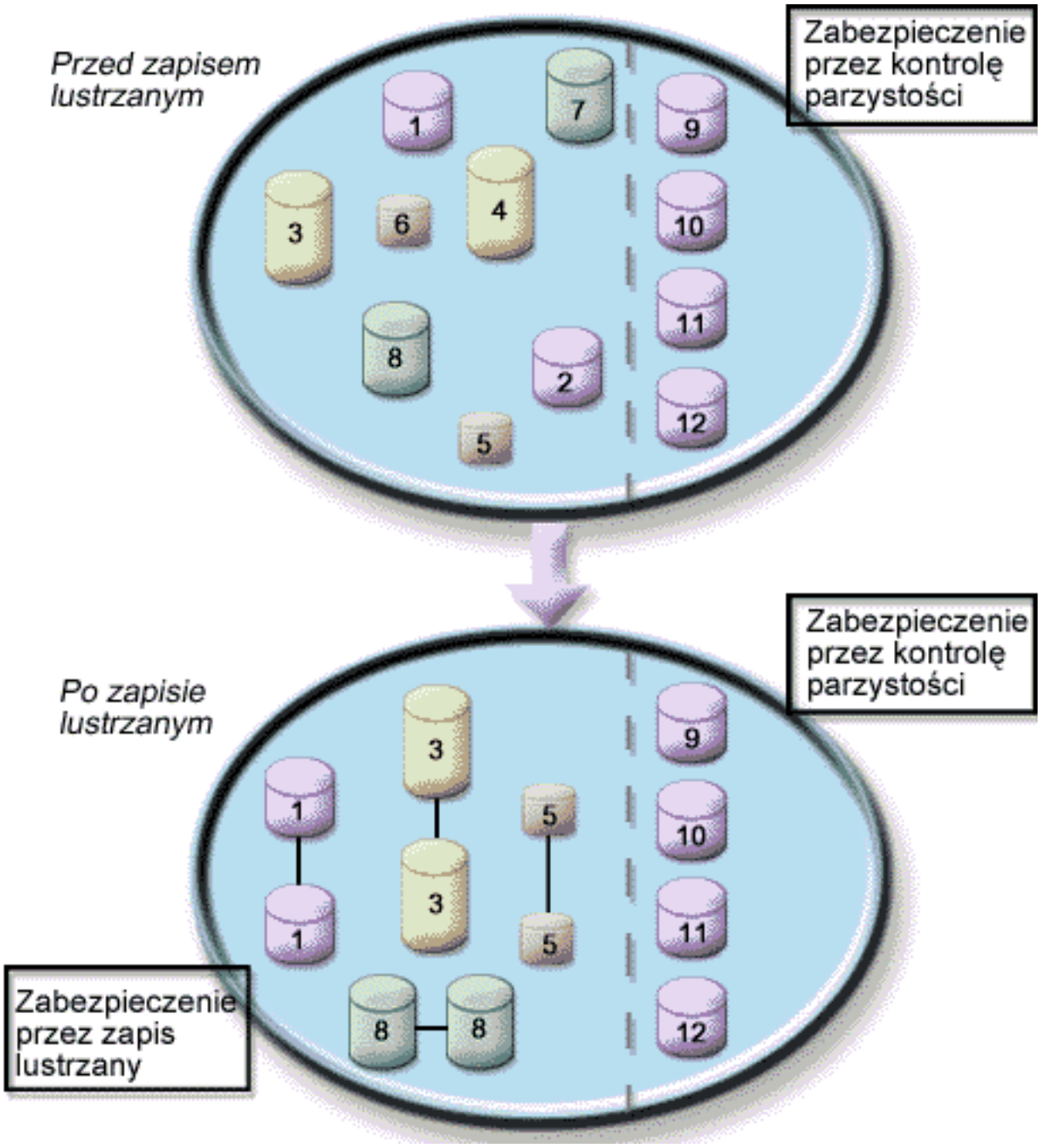
- Jak działa sprzętowe zabezpieczenie przez kontrolę parzystości
- Przykłady zabezpieczenia pul dyskowych przez kontrolę parzystości i przez zapis lustrzany

### Przykłady zabezpieczenia pul dyskowych przez kontrolę parzystości i przez zapis lustrzany

#### Zastosowanie zabezpieczenia przez zapis lustrzany i sprzętowego zabezpieczenia przez kontrolę parzystości do ochrony systemowej puli dyskowej

Poniżej przedstawiono przykład systemu z pojedynczą pulą dyskową (pulą pamięci dyskowej)

posiadającego zabezpieczenie przez zapis lustrzany i sprzętowe zabezpieczenie przez kontrolę parzystości.




Rysunek przedstawia pojedynczą pulę dyskową z dwunastoma jednostkami dyskowymi. Jednostki dyskowe 9–12 mają taką samą pojemność i są zabezpieczone przez sprzętową kontrolę parzystości. Jednostki dyskowe 1–8 mają różne pojemności, ale każda jednostka dyskowa po włączeniu zabezpieczenia przez zapis lustrzany może być połączona w parę z inną jednostką dyskową o tej samej pojemności. Po uruchomieniu zabezpieczenia przez zapis lustrzany jednostki dyskowe połączone w pary są identyfikowane na podstawie tego samego numeru; jednostki dyskowe 1 i 2 mają numer 1, i tak dalej. Gdy jedna z jednostek dyskowych ze sprzętowym zabezpieczeniem przez kontrolę parzystości ulegnie awarii, system pracuje nadal. W tym czasie uszkodzona jednostka może zostać naprawiona. Jeśli awaria nastąpi w jednostce dyskowej, która jest zabezpieczona przez zapis lustrzany, system działa nadal, wykorzystując sprawną jednostkę w lustrzanej parze.

**Zabezpieczenie przez zapis lustrzany w systemowej puli dyskowej i sprzętowe zabezpieczenie przez kontrolę parzystości w pulach dyskowych użytkowników**
Należy rozważyć zastosowanie sprzętowego zabezpieczenia przez kontrolę parzystości, jeśli w systemowej puli dyskowej istnieje zabezpieczenie przez zapis lustrzany i użytkownik zamierza utworzyć podstawowe lub niezależne pule dyskowe. System może tolerować awarie w jednej z jednostek dyskowych w podstawowej lub niezależnej puli dyskowej. Awarię można usunąć w czasie działania systemu.

**Zabezpieczenie przez zapis lustrzany i sprzętowe zabezpieczenie przez kontrolę parzystości we wszystkich pulach dyskowych**
Jeśli we wszystkich pulach dyskowych (pulach pamięci dyskowej) istnieje zabezpieczenie przez zapis lustrzany i użytkownik chce dodać jednostki do istniejących pul dyskowych, należy również wziąć pod uwagę użycie sprzętowego zabezpieczenia przez kontrolę parzystości. System może tolerować awarię w jednej z jednostek dyskowych ze sprzętowym zabezpieczeniem przez kontrolę parzystości. Uszkodzona jednostka może zostać naprawiona podczas normalnej pracy systemu. Jeśli awaria nastąpi w jednostce dyskowej, która jest zabezpieczona przez zapis lustrzany, system działa dalej, wykorzystując sprawną jednostkę w lustrzanej parze.

## Jak działa sprzętowe zabezpieczenie przez kontrolę parzystości
Po uruchomieniu zabezpieczenia przez kontrolę parzystości adaptery IOA tworzą zestawy parzystości urządzeń. Począwszy od adapterów wejścia/wyjścia (IOA) w wersji V5R2 minimalna liczba jednostek dyskowych w zestawie parzystości wynosi 3; maksymalna liczba jednostek dyskowych w zestawie parzystości wynosi 18. W przypadku adapterów wejścia/wyjścia (IOA) w wersjach wcześniejszych niż V5R2 minimalna liczba jednostek dyskowych w zestawie parzystości wynosi 4; maksymalna liczba jednostek dyskowych w zestawie parzystości wynosi 10. Zestaw parzystości może tolerować tylko awarię jednego dysku. Jeśli awarii ulegnie więcej niż jeden dysk, należy odtworzyć dane z nośnika składowania. Z powodu bardziej skomplikowanego zapisu odtwarzanie danych do puli dyskowej mającej jednostki dyskowe ze sprzętową kontrolą parzystości może zająć więcej czasu niż do puli dyskowej zawierającej tylko niechronione jednostki dyskowe.

W każdym zestawie parzystości odpowiednik jednej jednostki dyskowej jest odpowiedzialny za przechowywanie danych parzystości. Liczba jednostek dyskowych, które zawierają dane parzystości, zmienia się w zależności od liczby jednostek dyskowych w zestawie parzystości. Poniższa tabela określa liczbę jednostek dyskowych w każdym zestawie parzystości:

| Liczba jednostek dyskowych w zestawie parzystości | Liczba jednostek dyskowych zawierających dane parzystości |
|---|---|
| 3 | 2 |
| 4–7 | 4 |
| 8–15 | 8 |
| 16–18 | 16 |

Adapter we/wy określa liczbę formowanych zestawów parzystości. W adapterach w wersji V5R2 i nowszych użytkownik ma możliwość wyboru sposobu optymalizacji zestawu parzystości. Można optymalizować zestaw pod kątem *pojemności*, *wydajności* lub *obciążenia*. Jeśli optymalizacja przebiega pod kątem pojemności, adapter IOA próbuje utworzyć zestawy parzystości z większą liczbą jednostek dyskowych. Obszar używany do przechowywania danych użytkownika zostanie zwiększony, ale wydajność może nie być tak wysoka. Jeśli optymalizacja przebiega pod kątem wydajności, adapter IOA próbuje utworzyć zestaw parzystości z mniejszą liczbą jednostek dyskowych. Powinno to wpłynąć na zwiększenie szybkości operacji zapisu i odczytu, ale może również znacznie zwiększyć część dysku przeznaczoną na przechowywanie danych parzystości.

Tuż po uruchomieniu zabezpieczenia przez sprzętową kontrolę parzystości możliwe jest dołączenie do zestawu parzystości dodatkowych jednostek dyskowych o tej samej pojemności. Jednocześnie można dołączyć maksymalnie dwie jednostki dyskowe; jednak dla trzech lub więcej jednostek dyskowych system wymaga uruchomienia nowego zestawu parzystości zamiast dołączenia ich do istniejącego zestawu

parzystości. W iSeries Navigator można przeglądać właściwości każdej jednostki dyskowej. Jeśli statusem jednostki dyskowej jest *niezabezpieczona*, to znaczy, że nie jest ona zabezpieczona ani przez sprzętową kontrolę parzystości, ani przez zapis lustrzany i można ją dołączyć do istniejącego lub nowego zestawu parzystości. Można również wykluczyć dyski, które nie zawierają danych parzystości z zestawu parzystości bez zatrzymywania zabezpieczenia przez sprzętową kontrolę parzystości. Taka możliwość istnieje dla modeli numer 050 (lub 060, jeśli jest to skompresowana jednostka dyskowa). *Zabezpieczoną* jednostkę w modelu o numerze 070 (lub 080, jeśli jest to skompresowana jednostka dyskowa) można wykluczyć, ponieważ jest to jednostka dyskowa, która nie zawiera danych parzystości.

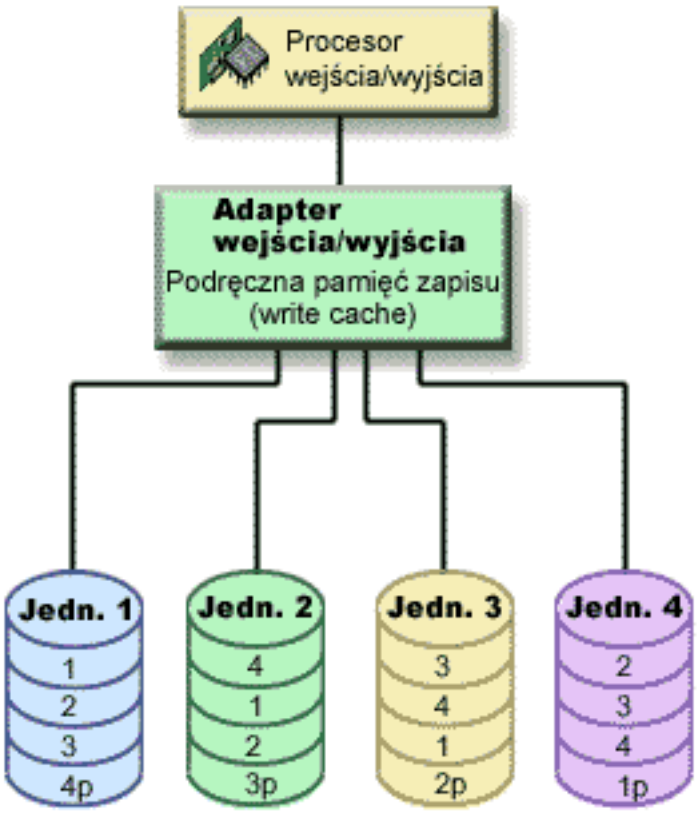
Jeśli wielkość zestawu parzystości rośnie, można wziąć pod uwagę redystrybucję danych parzystości. Można na przykład zacząć od 7 lub mniejszej liczby jednostek dyskowych, a następnie rozszerzyć zestaw parzystości do 8 lub większej liczby jednostek dyskowych. Aby poprawić wydajność zestawu z kontrolą parzystości, należy zatrzymać sprzętowe zabezpieczenie przez kontrolę parzystości i ponownie je uruchomić. Powoduje to redystrybucję danych parzystości w generalnie 8 dyskach, a nie w 4. Rozsyłanie danych parzystości do większej liczby jednostek dyskowych wpływa generalnie na wzrost wydajności.

Dla każdego zestawu parzystości w celu zwiększenia wydajności interaktywnych zadań zapisu dołączono do adaptera we/wy (IOA) pomięć podręczną zapisu. Sekcja Elementy sprzętowego zabezpieczenia przez kontrolę parzystości zawiera przykład zestawu parzystości z czterema jednostkami dyskowymi.

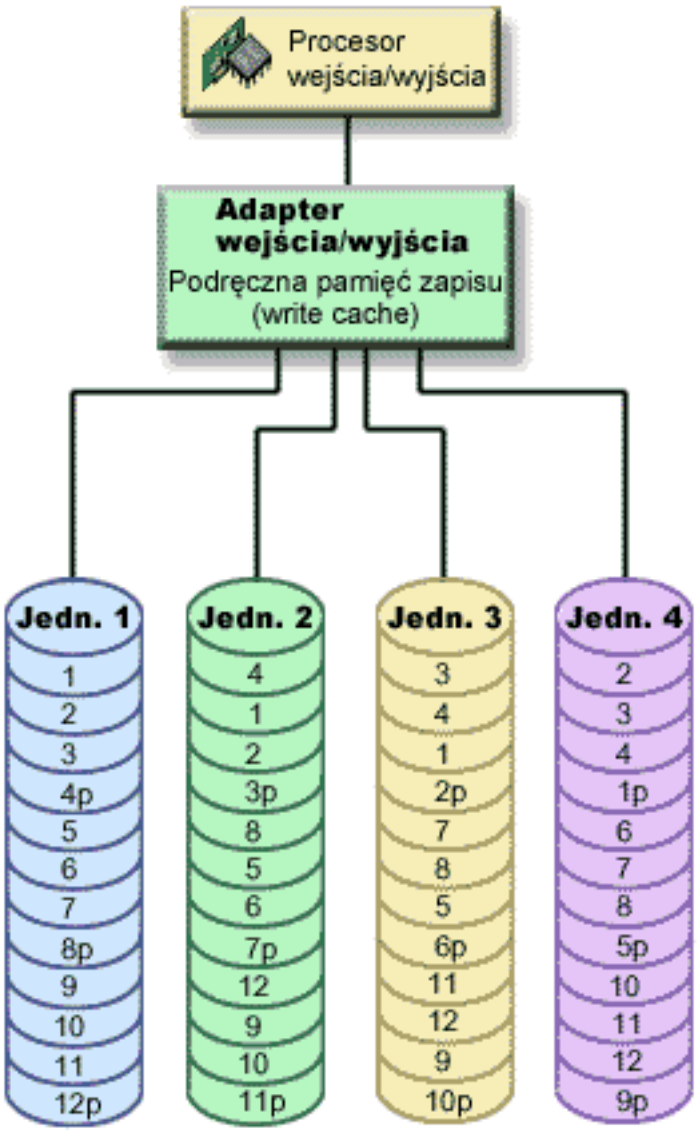
Począwszy od wersji V5R2, wszystkie adaptery we/wy (IOA) mogą obsługiwać zabezpieczenie przez sprzętową kontrolę parzystości. Jeśli użytkownik dysponuje wcześniejszym modelem adaptera, należy sprawdzić, czy może on obsługiwać zabezpieczenie przez sprzętową kontrolę parzystości. Więcej informacji na temat zmiany adaptera na model nowszej generacji zawiera sekcja Migrowanie do nowego adaptera wejścia/wyjścia.

**Uwaga:** Jeśli jest to możliwe, należy uruchomić sprzętowe zabezpieczenie przez kontrolę parzystości przed dodaniem jednostek dyskowych do puli dyskowej. Skraca to znacznie czas potrzebny na konfigurowanie jednostek dyskowych.

***Elementy sprzętowego zabezpieczenia przez kontrolę parzystości:*** Poniższe diagramy przedstawiają elementy zestawu parzystości zawierającego cztery jednostki dyskowe. Każdy zestaw parzystości otwiera procesor IOP, który jest podłączony do adaptera IOA, zawierającego pamięć podręczną zapisu. Adapter IOA przesyła sygnały odczytu i zapisu do podłączonych jednostek dyskowych. Pierwszy rysunek przedstawia sposób rozmieszczenia parzystości w adapterach, w wersjach wcześniejszych niż V5R2. Drugi rysunek przedstawia sposób rozmieszczenia parzystości w adapterach, w wersjach V5R2 i nowszych.




*Rysunek 1. Przykład rozmieszczenia danych parzystości w adapterach IOA w wersjach wcześniejszych niż V5R2*




*Rysunek 2. Przykład dystrybucji danych parzystości w adapterach IOA w wersji V5R2 i nowszych*

W przedstawionych przykładach *p* oznacza sekcje dysków, które zawierały dane parzystości. Pierwszy rysunek przedstawia przykład adaptera IOA w wersji wcześniejszej niż V5R2, w którym dane parzystości rozmieszczane są w jednej dużej porcji w każdej jednostce dyskowej zawierającej te dane. Drugi rysunek przedstawia, jak adaptery IOA w wersji V5R2 i nowsze rozmieszczają dane parzystości w jednostkach dyskowych w kilku dużych porcjach. Wydajność można zwiększyć poprzez rozsyłanie danych parzystości przez każdą z jednostek dyskowych.

Pamięć podręczna zapisu zapewnia większą integrację danych i większą wydajność. Gdy serwer iSeries wykonuje operację zapisu, dane są zapisywane do pamięci podręcznej. Następnie system otrzymuje komunikat informujący o zakończeniu zapisu. W tym momencie dane są zapisywane na dysk. Pamięć podręczna zapewnia szybszy zapis i zapewnia integralność danych.

Aby uzyskać więcej informacji, należy przejrzeć dodatkowe dane na temat pamięci podręcznej zapisu przedstawione powyżej.

*Podręczna pamięć zapisu (write cache):* Podczas żądania zapisu z serwera wykonywane są następujące działania:

1. Zatwierdzenie danych w nieulotnej, podtrzymywanej akumulatorem pamięci podręcznej znajdującej się w adapterze IOA.
2. Wysłanie z serwera komunikatu o zakończeniu operacji zapisu.

Po wysłaniu komunikatu o zakończeniu operacji zapisu wykonywane są następujące działania:

1. Wysłanie operacji zapisu z pamięci podręcznej adaptera IOA do jednostki dyskowej.
   - Dla dysku danych operacja ta:
     - odczytuje oryginalne dane,
     - oblicza różnicę parzystości przez porównanie nowych i początkowych danych,
     - zapisuje nowe dane.
   - Dla dysku parzystości operacja ta:
     - odczytuje oryginalną informację o parzystości,
     - oblicza nową parzystość przez porównanie różnicy parzystości i parzystości początkowej,
     - zapisuje nowe informacje o parzystości.
2. Oznaczenie danych jako zatwierdzonych następuje w momencie, gdy są poprawnie zapisane zarówno do jednostki dyskowej danych, jak i do jednostki dyskowej parzystości.

Wydajność tego typu operacji zapisu zależy od rywalizacji dysków i czasu potrzebnego na obliczenie parzystości.

## Migrowanie do nowego adaptera we/wy

Przed migrowaniem do nowego adaptera we/wy (IOA), podobnie jak w przypadku dowolnej zmiany w konfiguracji, ważne jest, aby normalnie wyłączyć system. Gwarantuje to, że wszystkie dane z pamięci podręcznej zostaną zeskładowane. Podczas migrowania istniejącego zestawu parzystości z adaptera IOA w wersji wcześniejszej niż V5R2 do wersji V5R2 lub nowszej jednostki dyskowe nie będą podczas regeneracji parzystości chronione za pomocą sprzętowego zabezpieczenia przez kontrolę parzystości.

**Uwaga:**
Nie można migrować zestawu parzystości z powrotem do starej generacji adapterów po wprowadzeniu zmian wymaganych przez nowy adapter. Jeśli pojawi się wzmiankowana potrzeba, należy zatrzymać sprzętowe zabezpieczenie przez kontrolę parzystości, powiązać dyski ze starym adapterem i zrestartować sprzętowe zabezpieczenie przez kontrolę parzystości.

## Sprzętowe zabezpieczenie przez kontrolę parzystości – korzyści

Oto korzyści, jakie daje sprzętowe zabezpieczenie przez kontrolę parzystości:

- po awarii dysku utracone dane są automatycznie odzyskiwane przez kontroler dysku,
- po awarii pojedynczego dysku system nadal pracuje,
- uszkodzona jednostka dyskowa może zostać wymieniona bez zatrzymywania systemu,
- sprzętowe zabezpieczenie przez kontrolę parzystości zmniejsza liczbę obiektów uszkodzonych w wyniku uszkodzenia dysku,
- tylko 1 jednostka dyskowa pojemności przechowuje dane parzystości w zestawie parzystości.

## Sprzętowe zabezpieczenie przez kontrolę parzystości – koszty i ograniczenia

Oto koszty i ograniczenia, jakie niesie ze sobą sprzętowe zabezpieczenie przez kontrolę parzystości:

- Sprzętowe zabezpieczenie przez kontrolę parzystości może wymagać dodatkowych jednostek dyskowych, aby zapobiec zmniejszeniu wydajności.
- Podczas stosowania sprzętowego zabezpieczenia przez kontrolę parzystości, operacje odtwarzania mogą trwać dłużej.

## Wpływ sprzętowego zabezpieczenia przez kontrolę parzystości na wydajność

Sprzętowe zabezpieczenie przez kontrolę parzystości wymaga dodatkowych operacji do zapisania danych o parzystości. Aby uniknąć problemów z wydajnością, wszystkie adaptery IOA zawierają nieulotną pamięć podręczną zapisu zapewniającą integralność danych i szybszy zapis. System jest powiadamiany o zakończeniu operacji zapisu, gdy tylko dane zostaną zapisane w pamięci podręcznej. Dane są gromadzone w pamięci podręcznej przed ich zapisaniem na jednostkę dyskową. Redukuje to liczbę fizycznych operacji zapisu na jednostce dyskowej. Dzięki zastosowaniu pamięci podręcznej wydajność zabezpieczonych i niezabezpieczonych jednostek dyskowych jest praktycznie taka sama.

Aplikacje wykonujące wiele operacji zapisu w krótkim czasie, takie jak zadania wsadowe, mogą niekorzystnie wpłynąć na wydajność. Awaria pojedynczej jednostki dyskowej może niekorzystnie wpłynąć na wydajność zarówno operacji zapisu, jak i odczytu.

Dodatkowe przetwarzanie wynikające z awarii jednostki dyskowej w zestawie z kontrolą parzystości może mieć istotne znaczenie. Spadek wydajności jest widoczny aż do momentu naprawy (lub wymiany) uszkodzonej jednostki i zakończenia procesu odbudowy. Jeśli sprzętowe zabezpieczenie przez kontrolę parzystości zbyt mocno obniża wydajność, należy rozważyć zastosowanie zabezpieczenia przez zapis lustrzany. Poniższe sekcje zawierają szczegółowe informacje o wpływie awarii jednostki dyskowej na wydajność:

- Awaria jednostki dyskowej w konfiguracji ze sprzętowym zabezpieczeniem przez kontrolę parzystości
- Operacje odczytu z uszkodzonej jednostki dyskowej
- Operacje zapisu na uszkodzoną jednostkę dyskową
- Operacje wejścia/wyjścia podczas procesu odbudowy

### Awaria jednostki dyskowej w konfiguracji ze sprzętowym zabezpieczeniem przez kontrolę parzystości

Jeśli jednostka dyskowa ulegnie awarii, podsystemy ze sprzętowym zabezpieczeniem przez kontrolę parzystości będą narażone na niebezpieczeństwo aż do momentu zakończenia procesu synchronizacji po wymianie uszkodzonej jednostki dyskowej. W czasie gdy jednostka dyskowa jest uznawana za narażoną na niebezpieczeństwo, wymagane są dodatkowe operacje wejścia/wyjścia. Jeśli druga jednostka dyskowa ulegnie awarii, dane należy odtworzyć z nośnika składowania.

### Operacje odczytu z uszkodzonej jednostki dyskowej

Aby odzyskać dane zawarte na uszkodzonej jednostce dyskowej, układ sprzętowego zabezpieczenia przez kontrolę parzystości musi odczytać dane z każdej jednostki dyskowej w zestawie z kontrolą parzystości zawierającym uszkodzoną jednostkę dyskową. Ponieważ operacje odczytu mogą się nakładać, spadek wydajności może być niewielki.

Ponieważ uszkodzona jednostka dyskowa ze sprzętowym zabezpieczeniem przez kontrolę parzystości może zawierać małą ilość danych użytkowników, jest możliwe, że obniżenie wydajności będzie dotyczyło tylko kilku użytkowników.

### Operacje zapisu na uszkodzoną jednostkę dyskową

Poniżej umieszczono kilka przykładów ilustrujących, co dzieje się podczas operacji zapisu w przypadku uszkodzenia pojedynczej jednostki dyskowej ze sprzętowym zabezpieczeniem przez kontrolę parzystości. Poniższy rysunek przedstawia uszkodzoną jednostkę w adapterze IOA ze sprzętowym zabezpieczeniem przez kontrolę parzystości. Należy go użyć w następujących przykładach:

- Przykład: zapis danych na uszkodzoną jednostkę dyskową
- Przykład: zapis danych na jednostkę dyskową, gdy w uszkodzonej jednostce dyskowej są odpowiednie dane parzystości


*Rysunek 3. Zestaw sprzętowej parzystości z uszkodzoną jednostką dyskową*

Rysunek przedstawia zestaw parzystości z czterema jednostkami dyskowymi. Każda sekcja jednostki dyskowej jest oznaczona dwoma numerami. Sektory parzystości są oznaczane jako *p*. Jednostka dyskowa 3 jest uszkodzona. Jednostka dyskowa 1 zawiera sektory 1, 2, 3 i 4p. Jednostka dyskowa 2 zawiera sektory 4, 1, 2 i 3p. Uszkodzona jednostka dyskowa 3 zawiera sektory 3, 4, 1 i 2p. Jednostka dyskowa 4 zawiera sektory 2, 3, 4 i 1p.

***Przykład: zapis danych na uszkodzoną jednostkę dyskową:*** Podczas operacji zapisu z serwera iSeries okazało się, że jednostka dyskowa, która ma zawierać dane, jest uszkodzona. Operacja zapisu ma zostać wykonana na jednostce dyskowej 3, w sektorze 1. Wykonane zostaną następujące działania:

1. Z powodu awarii utracone zostaną dane z jednostki dyskowej 3, sektora 1.
2. Nowe dane parzystości są obliczane poprzez odczyt jednostki dyskowej 1, sektora 1 oraz jednostki dyskowej 2, sektora 1.
3. Obliczana jest nowa wartość parzystości.
4. Z powodu awarii nie można zapisać nowych danych do sektora 1 w jednostce dyskowej 3.
5. Nowe dane parzystości są zapisywane do sektora parzystości 1 w jednostce dyskowej 4.

   Operacja zapisu nowych danych parzystości wymaga kilku odczytów (N-2 odczytów, gdzie N jest liczbą jednostek dyskowych) oraz tylko jednej operacji zapisu. Dane z jednostki dyskowej 3 zostaną odtworzone podczas synchronizacji po wymianie jednostki dyskowej 3.

***Przykład: zapis danych na jednostkę dyskową, gdy w uszkodzonej jednostce dyskowej są odpowiednie dane parzystości:*** Żądanie zapisu z serwera iSeries wykrywa awarię dysku dla jednostki dyskowej zawierającej odpowiednie dane parzystości. Żądanie zapisu dotyczy sektora 2 w jednostce dyskowej 4. Informacje o parzystości dla jednostki dyskowej 4, sektora 2, znajdują się w uszkodzonej jednostce dyskowej 3. Wykonane zostaną poniższe działania:

1. Wykrycie awarii w jednostce dyskowej 3 zawierającej dane parzystości.
2. Obliczanie informacji parzystości nie jest konieczne, ponieważ nie można ich zapisać do sektora parzystości 2 jednostki dyskowej 3. Dlatego nie ma wymogu odczytu oryginalnych danych i informacji o parzystości.
3. Zapisanie danych do jednostki dyskowej 4, sektora 2.

   Operacja zapisu wymaga tylko jednego zapisu dla nowych danych. Dane parzystości dla sektora parzystości 2 w jednostce dyskowej 3 zostaną odbudowane podczas synchronizacji po wymianie jednostki dyskowej 3.

### Operacje wejścia/wyjścia podczas procesu odbudowy

Operacje wejścia/wyjścia w czasie procesu odbudowy (synchronizacji) uszkodzonej jednostki dyskowej zazwyczaj nie wymagają dodatkowych żądań wejścia/wyjścia dla dysku. Zależy to od tego, skąd dane są odczytywane lub gdzie są zapisywane na jednostkę dyskową, która jest w trakcie synchronizacji. Na przykład:

- Operacja odczytu z obszaru dysku, który już został odbudowany, wymaga jednej operacji odczytu.
- Operacja odczytu z obszaru dysku, który nie został jeszcze odbudowany, jest traktowana jako operacja odczytu z uszkodzonej jednostki dyskowej. Dalsze informacje zawiera sekcja Operacje odczytu z uszkodzonej jednostki dyskowej.
- Operacja zapisu na dysk, który już został odbudowany, wymaga normalnych operacji odczytu i zapisu (dwie operacje odczytu i dwie operacje zapisu).
- Operacja zapisu do obszaru, który nie został jeszcze odbudowany, jest traktowana jako operacja zapisu na uszkodzoną jednostkę dyskową. Dalsze informacje zawiera sekcja Operacje zapisu na uszkodzoną jednostkę dyskową.

**Uwaga:** Proces odbudowy trwa dłużej, gdy przeprowadzane są operacje odczytu i zapisu na uszkodzoną jednostkę. Każde żądanie odczytu lub zapisu przerywa proces odbudowy w celu wykonania żądanej operacji.

## Łączne użycie sprzętowego zabezpieczenia przez kontrolę parzystości i zabezpieczenia przez zapis lustrzany

Sprzętowe zabezpieczenie przez kontrolę parzystości jest funkcją sprzętową. Pule dyskowe i zabezpieczenie przez zapis lustrzany są funkcjami oprogramowania. Podczas dodawania jednostek dyskowych i uruchamiania sprzętowego zabezpieczenia przez kontrolę parzystości podsystem dyskowy lub IOP nie zawiera informacji o jakiejkolwiek programowej konfiguracji dla jednostek dyskowych. Oprogramowanie obsługujące zabezpieczenie dysków zawiera informacje o jednostkach, które mają sprzętowe zabezpieczenie przez kontrolę parzystości.

Poniższe reguły i uwagi mają zastosowanie przy łączeniu sprzętowego zabezpieczenia przez kontrolę parzystości z zabezpieczeniem przez zapis lustrzany:

- Sprzętowego zabezpieczenia przez kontrolę parzystości nie implementuje się jednostkom znajdującym się w różnych pulach dyskowych.
- Zabezpieczenie przez zapis lustrzany jest implementowane jednostkom znajdującym się w różnych pulach dyskowych.
- Można uruchomić zabezpieczenie przez zapis lustrzany dla puli dyskowej, nawet jeśli nie zawiera ona jednostek, które są dostępne dla takiego zabezpieczenia, ponieważ wszystkie te jednostki mają sprzętowe zabezpieczenie przez kontrolę parzystości. Gwarantuje to, że pula dyskowa zawsze będzie w pełni chroniona, nawet jeśli w późniejszym terminie dodane zostaną jednostki dyskowe bez sprzętowego zabezpieczenia przez kontrolę parzystości.
- Jednostka dyskowa dodawana do konfiguracji systemu może mieć sprzętowe zabezpieczenie przez kontrolę parzystości, ale nie musi.
- W przypadku w pełni zabezpieczonego systemu należy całkowicie chronić wszystkie pule dyskowe, za pomocą sprzętowego zabezpieczenia przez kontrolę parzystości lub zabezpieczenia przez zapis lustrzany albo obu tych zabezpieczeń jednocześnie.
- Jednostki dyskowe chronione za pomocą sprzętowego zabezpieczenia przez kontrolę parzystości można dodawać do puli dyskowej z zabezpieczeniem przez zapis lustrzany. Jednostki dyskowe, które mają sprzętowe zabezpieczenie przez kontrolę parzystości, nie biorą udziału w zabezpieczeniu przez zapis lustrzany. Sprzęt już je zabezpiecza.
- Po dodaniu jednostki dyskowej, która nie jest chroniona przez sprzętowe zabezpieczenie przez kontrolę parzystości, do puli dyskowej mającej zabezpieczenie przez zapis lustrzany, nowa jednostka dyskowa bierze udział w zabezpieczeniu przez zapis lustrzany. Jednostki dyskowe muszą być dodawane i usuwane z lustrzanej puli dyskowej w parach o równej pojemności.

- Przed uruchomieniem sprzętowego zabezpieczenia przez kontrolę parzystości dla skonfigurowanych jednostek dyskowych (przypisanych do puli dyskowej), należy zatrzymać zabezpieczenie przez zapis lustrzany dla puli dyskowej.
- Przed zatrzymaniem sprzętowego zabezpieczenia przez kontrolę parzystości należy zatrzymać zabezpieczenie przez zapis lustrzany dla wszystkich pul dyskowych zawierających odpowiednie jednostki dyskowe.
- Gdy zabezpieczenie przez zapis lustrzany zostanie zatrzymane, jedna jednostka dyskowa z każdej pary lustrzanej stanie się nieskonfigurowana. Nieskonfigurowane jednostki dyskowe należy ponownie dodać do puli dyskowej przed uruchomieniem zabezpieczenia przez zapis lustrzany.

## Zabezpieczenie przez zapis lustrzany

Zabezpieczenie przez zapis lustrzany jest funkcją programową, która zabezpiecza przed utratą danych w wyniku awarii lub uszkodzenia dysku. Dane są chronione dzięki temu, że system tworzy dwie kopie danych na dwóch osobnych jednostkach dyskowych. Kiedy element związany z dyskiem ulegnie uszkodzeniu, system może kontynuować pracę bez zatrzymywania się, korzystając z lustrzanej kopii danych aż do momentu usunięcia awarii uszkodzonego elementu.

Po uruchomieniu zabezpieczenia przez zapis lustrzany lub dodaniu jednostek dyskowych do puli dyskowej z zabezpieczeniem przez zapis lustrzany system tworzy lustrzane pary używając jednostek dyskowych o takiej samej pojemności. Celem nadrzędnym jest ochrona tak wielu elementów powiązanych z dyskami, jak jest to tylko możliwe. Aby zapewnić maksymalną nadmiarowość sprzętu i zabezpieczenie, system próbuje tworzyć pary jednostek dyskowych podłączonych do różnych kontrolerów, adapterów we/wy, procesorów we/wy, magistral i wież.

Zabezpieczenie przez zapis lustrzany ma na celu ochronę przed utratą danych w przypadku awarii dysku. Jest ono funkcją programową, która używa duplikatów elementów systemu dyskowego w celu utrzymania dostępności systemu, jeśli jeden ze składników zawiedzie. Zabezpieczenie, które jest częścią Licencjonowanego Kodu Wewnętrznego, może być używane w dowolnym modelu serwera iSeries.

W zależności od tego, jaki psrzęt jest duplikowany, możliwe są różne wersje zabezpieczenia przez zapis lustrzany. Można duplikować:
- jednostki dyskowe,
- adaptery we/wy,
- procesory we/wy,
- magistrale,
- wieże,
- szybkie połączenia.

System pozostanie dostępny po wystąpieniu awarii wówczas, jeśli uszkodzony element oraz dołączone do niego elementy sprzętu zostały duplikowane. Dalsze szczegóły techniczne opisujące pamięć serwera oraz zabezpieczenie przez zapis lustrzany zawierają sekcje Jak serwer adresuje pamięć oraz Zabezpieczenie przez zapis lustrzany – jak to działa.

Zdalny zapis lustrzany umożliwia takie tworzenie par lustrzanych, w którym jedna jednostka lustrzana znajduje się w miejscu lokalnym, a druga w miejscu zdalnym. W przypadku niektórych systemów standardowy zapis lustrzany DASD pozostaje najlepszym rozwiązaniem. W przypadku innych zdalny zapis lustrzany DASD daje cenne dodatkowe możliwości. Przed podjęciem decyzji o wyborze typu zapisu należy ustalić potrzeby systemu, wziąć pod uwagę korzyści i wady wszystkich typów zapisu lustrzanego, a następnie zdecydować, które rozwiązanie jest lepsze.

Dalsze informacje opisujące zabezpieczenie przez zapis lustrzany znajdują się w poniższych sekcjach:
- Zabezpieczenie przez zapis lustrzany – korzyści
- Zabezpieczenie przez zapis lustrzany – koszty i ograniczenia
- Planowanie zabezpieczenia przez zapis lustrzany

- Zabezpieczenie przez zdalny zapis lustrzany DASD

Więcej informacji na temat implementacji zabezpieczenia przez zapis lustrzany zawiera książka Składowanie i odtwarzanie. 

## Zabezpieczenie przez zapis lustrzany – korzyści

Jeśli zabezpieczenie przez zapis lustrzany jest dobrze skonfigurowane, system działa bez przerwy po wystąpieniu awarii sprzętu dyskowego. W przypadku niektórych jednostek systemu uszkodzenia mogą być usuwane bez konieczności wyłączania systemu. Jeśli elementu nie można wymienić lub naprawić w czasie działania systemu (magistrala lub procesor I/O), system zwykle może działać po wystąpieniu awarii. Naprawa może zostać odłożona i można normalnie wyłączyć system. Unika się w ten sposób długiego czasu odzyskiwania.

Nawet jeśli system nie jest duży, zabezpieczenie przez zapis lustrzany może mieć sporo zalet. Uszkodzenie dysku lub innego tego typu sprzętu w systemie niezabezpieczonym może spowodować jego wyłączenie na wiele godzin. Rzeczywisty czas zależy od rodzaju awarii, wielkości jednostki pamięci, strategii składowania, szybkości jednostki taśm, typu i intensywności wykonywanego przez system przetwarzania. Jeśli rodzaj wykonywanej działalności wyklucza możliwość tolerowania tego typu utraty dostępności, należy rozważyć zabezpieczenie systemu przez zapis lustrzany niezależnie od jego wielkości.

## Zabezpieczenie przez zapis lustrzany – koszty i ograniczenia

Podstawowy koszt użycia zabezpieczenia przez zapis lustrzany dotyczy sprzętu. Aby uzyskać wysoką dostępność i uniknąć utraty danych po awarii jednostki dyskowej, należy zabezpieczyć wszystkie pule dyskowe przez zapis lustrzany. Zwykle wymaga to dwukrotnie większej liczby jednostek dyskowych. Jeśli chce się uniknąć utraty danych i przerwania ciągłości działania w przypadku wystąpienia awarii jednostki dyskowej, kontrolera lub IOP, należy zduplikować kontrolery dysków i procesory I/O. Można przeprowadzić modernizację modelu w celu prawie całkowitego uniknięcia utraty danych i przerwania ciągłości działania systemu w przypadku wystąpienia jednego z powyższych uszkodzeń, w tym awarii magistrali. System nie będzie mógł, niestety, działać w przypadku uszkodzenia magistrali 1. Ponieważ jednak awarie magistrali występują rzadko, a zabezpieczenie na poziomie magistrali nie jest znacząco większe od zabezpieczenia na poziomie IOP, modernizacja modelu może okazać się nieefektywna z punktu widzenia kosztów i potrzeb.

Zabezpieczenie przez zapis lustrzany ma niewielki wpływ na wydajność. Ponieważ magistrale, procesory I/O i kontrolery nie są bardziej obciążone w systemach z zabezpieczeniem przez zapis lustrzany niż w równoważnych systemach bez zabezpieczenia, wydajność obu systemów powinna być w przybliżeniu jednakowa.

Przy podejmowaniu decyzji o użyciu zabezpieczenia przez zapis lustrzany należy porównać koszty potencjalnych wyłączeń systemu i koszty dodatkowego sprzętu, a także czas życia systemu. Koszty ewentualnej utraty wydajności lub złożoność systemu są zwykle nieistotne. Trzeba również wziąć pod uwagę możliwość zastosowania innych zabezpieczeń; należy do nich, na przykład, sprzętowe zabezpieczenie przez kontrolę parzystości. Zabezpieczenie przez zapis lustrzany wymaga dwukrotnego zwiększenia pamięci dyskowej. Ze względu na obsługę techniczną w trakcie pracy systemu oraz wysoką dostępność systemów zabezpieczonych przez zapis lustrzany może być potrzebny dodatkowy sprzęt.

### Ograniczenia

Chociaż zabezpieczenie przez zapis lustrzany może zapewnić ciągłość pracy systemu w razie wystąpienia awarii sprzętu związanego z dyskami, nie stanowi ono alternatywy dla procedury składowania. Istnieje wiele typów uszkodzeń sprzętu dyskowego lub katastrof (jak powódź czy akcja sabotażowa), w których konieczne jest zastosowanie nośnika składowania.

Zabezpieczenie przez zapis lustrzany nie zapewni ciągłości pracy systemu, jeśli pozostała po awarii jednostka pamięci również ulegnie uszkodzeniu, zanim ta pierwsza zostanie naprawiona i zabezpieczenie

zostanie przywrócone. Jeśli dwie uszkodzone jednostki pamięci znajdują się w dwóch różnych parach, system pozostaje dostępny i przeprowadzane jest normalne odzyskiwanie zabezpieczenia przez zapis lustrzany, ponieważ z punktu widzenia odzyskiwania pary lustrzane nie zależą od siebie. Jeśli nastąpi awaria drugiej jednostki pamięci z tej samej pary lustrzanej, uszkodzenie może nie spowodować utraty danych. Jeśli uszkodzenie dotyczy układów elektronicznych dysku lub jeśli do odzyskania wszystkich danych przedstawiciel serwisu może z powodzeniem użyć funkcji Składowanie danych jednostki dyskowej (Save Disk Unit Data), dane nie zostaną utracone.

Jeśli jednostki pamięci w parze lustrzanej ulegną awarii powodując utratę danych, cała pula dyskowa ulega utracie i zawartość wszystkich jednostek w puli dyskowej jest usuwana. Należy się przygotować do odtwarzania puli dyskowej z nośnika składowania oraz zastosować zmiany z kroniki.

Podczas uruchamiania zabezpieczenia przez zapis lustrzany obiekty tworzone na preferowanej jednostce mogą być przenoszone na inną jednostkę. Po uruchomieniu zabezpieczenia preferowana jednostka może przestać istnieć.

## Planowanie zabezpieczenia przez zapis lustrzany

W przypadku systemu z wieloma magistralami oraz dużego systemu z jedną magistralą należy rozważyć zabezpieczenie przez zapis lustrzany. Im więcej jest w systemie jednostek dyskowych, tym częstsze są uszkodzenia sprzętowe związane z dyskami. Jest po prostu więcej urządzeń, które mogą ulec awarii. Przy rosnącej liczbie jednostek pamięci wzrasta również znacząco czas potrzebny na odtworzenie danych po wystąpieniu uszkodzenia podsystemu sprzętu. Wraz ze wzrostem wielkości pamięci dyskowej w systemie rośnie także znacznie czas odzyskiwania po awarii pamięci dyskowej systemu. System jest częściej niedostępny, trwa to dłużej i jest bardziej kosztowne.

Uwzględniając zabezpieczenie przez zapis lustrzany należy skontaktować się z przedstawicielem handlowym IBM, aby uzyskać wskazówki dotyczące kolejnych kroków planowania i ułatwiające:
1. Określenie, które pule dyskowe mają być chronione.
2. Określenie liczby potrzebnych jednostek dyskowych.
3. Określenie wymaganego poziomu zabezpieczenia.
4. Określenie, jakiego dodatkowego sprzętu wymaga zabezpieczenie przez zapis lustrzany.
5. Określenie, jakiego dodatkowego sprzętu wymaga zachowanie dotychczasowej wydajności.
6. Zamówienie sprzętu.
7. Zaplanowanie instalacji sprzętu i konfigurowania nowych jednostek.
8. Zainstalowanie nowego sprzętu.

Dalsze informacje opisujące zabezpieczenie przez zapis lustrzany znajdują się w poniższych sekcjach:
- Zabezpieczenie przez zapis lustrzany – korzyści
- Zabezpieczenie przez zapis lustrzany – koszty i ograniczenia
- Zabezpieczenie przez zapis lustrzany – jak to działa

### Zabezpieczenie przez zapis lustrzany – jak to działa

Ponieważ zabezpieczenie przez zapis lustrzany jest skonfigurowane przez pulę dyskową, można utworzyć kopię lustrzaną jednej, kilku lub wszystkich pul dyskowych w systemie. Domyślnie każdy system ma systemową pulę dyskową. Nie trzeba tworzyć pul dyskowych użytkowników, aby używać zabezpieczenia przez zapis lustrzany. Chociaż zabezpieczenie przez zapis lustrzany jest skonfigurowane przez jednostkę dyskową, wszystkie pule dyskowe muszą być chronione przez zapis lustrzany w celu zapewnienia maksymalnej dostępności systemu. Jeśli jednostka dyskowa ulegnie awarii w puli dyskowej nieposiadającej ochrony przez zapis lustrzany, nie można używać systemu aż do momentu naprawy lub wymiany jednostki dyskowej.

Algorytm uruchamiania par lustrzanych wybiera taką konfigurację kopii lustrzanych, która daje maksymalne zabezpieczenie danej konfiguracji sprzętu w systemie na poziomie magistrali, IOP lub kontrolera. Gdy jednostki pamięci w jednej parze lustrzanej są podłączone do różnych magistral, ich zabezpieczenie jest

maksymalnie niezależne. Ponieważ żadne zasoby nie są udostępniane na poziomie magistrali, IOP lub kontrolera, w przypadku uszkodzenia jednego z tych elementów druga jednostka lustrzana może nadal działać.

Wszelkie dane zapisane na jednostce zabezpieczonej przez zapis lustrzany zachowywane są na obu jednostkach z pary lustrzanej. Odczytywanie danych odbywa się z jednej jednostki pamięci w parze. Użytkownik widzi, z której jednostki lustrzanej dane są odczytywane. Nie wie on o istnieniu dwu fizycznych kopii danych.

Jeśli jedna jednostka z pary lustrzanej ulegnie awarii, system *zawiesza* zabezpieczenie uszkodzonej jednostki przez zapis lustrzany. Działanie zabezpieczenia będzie kontynuowane na pozostałych jednostkach lustrzanych. Uszkodzenie jednostki lustrzanej może być fizycznie usunięte lub może zostać wymieniona sama jednostka.

Po naprawieniu lub zastąpieniu uszkodzonej jednostki lustrzanej system *synchronizuje* parę lustrzaną, kopiując aktualne dane z jednostki, która działała właściwie, na drugą jednostkę. W trakcie synchronizacji jednostka lustrzana, na którą kopiowane są informacje, znajduje się w stanie *przywracania*. Synchronizacja nie musi być przeprowadzana w trybie dedykowanym systemu i jest wykonywana równocześnie z innymi zadaniami. W czasie synchronizacji wydajność systemu spada. Po zakończeniu synchronizacji jednostka lustrzana staje się *aktywna*.

Szczegóły dotyczące pamięci w serwerze zawiera sekcja Jak serwer adresuje pamięć.

***Jak serwer adresuje pamięć:*** Jednostki dyskowe są przypisywane do puli dyskowej na podstawie jednostki pamięci. Każda jednostka pamięci w obrębie jednostki dyskowej traktowana jest jako oddzielna jednostka pamięci dyskowej. Kiedy do systemu dołączana jest nowa jednostka dyskowa, początkowo jej jednostki pamięci traktowane są jako nieskonfigurowane. Używając opcji narzędzi DST można dodać te nieskonfigurowane jednostki pamięci do systemowej puli dyskowej, podstawowej puli dyskowej lub niezależnej puli dyskowej. Dodając nieskonfigurowaną jednostkę pamięci, należy użyć numeru seryjnego dostarczonego przez producenta, aby wybrać właściwą fizyczną jednostkę dyskową. Dodatkowo pojedyncze jednostki pamięci w obrębie danej jednostki dyskowej mogą być identyfikowane za pomocą adresu uzyskanego z ekranu Wyświetlanie konfiguracji dysków (DST Display Disk Configuration).

Po dodaniu nieskonfigurowanej jednostki pamięci do puli dyskowej system przypisuje numer do jednostki pamięci. Numer jednostki może być używany zamiast numeru seryjnego i adresu. Ten sam numer jednostki używany jest dla wybranej jednostki pamięci nawet wtedy, kiedy jednostka dyskowa podłączana jest do systemu w inny sposób.

Kiedy jednostka jest zabezpieczona przez zapis lustrzany, dwie jednostki z pary lustrzanej mają ten sam numer jednostki. Natomiast numer seryjny i adres różnią się między sobą w przypadku jednostek pamięci z pary lustrzanej.

Aby później określić, jaki numer jednostki przypisany jest do fizycznej jednostki dyskowej, należy dla pewności zanotować numer przypisany jednostce. Jeśli istnieje dostęp do drukarki, należy wydrukować ekran DST lub SST konfiguracji dysków. Jeśli przypisanie numeru jednostki wymaga weryfikacji, można użyć ekranu statusu konfiguracji DST lub SST do wyświetlenia numerów seryjnych i adresów każdej jednostki.

Jednostkę pamięci, której przydzielony zostanie adres jednostki 1, system używa zawsze do przechowywania Licencjonowanego Kodu Wewnętrznego i obszarów danych. Ilość pamięci używanej przez jednostkę 1 jest dosyć duża i zależy od konfiguracji systemu. Jednostka 1 zawiera ograniczoną ilość danych użytkowników. Ponieważ jednostka 1 zawiera programy początkowe oraz dane potrzebne podczas IPL, jest nazywana **jednostką ładowania systemu**.

System rezerwuje stałą ilość pamięci na innych jednostkach, ograniczając dostępny na nich obszar. Wielkość tego obszaru wynosi 1,08 MB dla każdej jednostki.

***Zdalny zapis lustrzany:*** Obsługa zdalnego zapisu lustrzanego umożliwia podzielenie jednostek dyskowych systemu na grupy lokalnych DASD i grupy zdalnych DASD. Zdalne DASD są podłączone do jednego zestawu magistral optycznych. Lokalne DASD podłączone są do innego zestawu. Lokalne i zdalne DASD mogą być fizycznie rozdzielone i znajdować się w różnych serwerach. Poprowadzenie odpowiednich magistral optycznych do zdalnego serwera zwiększa poziom ochrony w razie awarii serwera.

***Obsługa techniczna w trakcie pracy systemu:*** Obsługa techniczna w trakcie pracy systemu jest to proces naprawy lub zastąpienia uszkodzonych elementów sprzętu związanych z dyskami podczas normalnej pracy systemu.

W systemach bez zabezpieczenia przez zapis lustrzany lub sprzętowego zabezpieczenia przez kontrolę parzystości w momencie wystąpienia awarii elementu sprzętowego związanego z dyskiem system jest niedostępny i pozostaje taki aż do naprawy lub usunięcia uszkodzonego elementu. Jeśli system jest zabezpieczony przez zapis lustrzany, awaria sprzętu może być często usuwana w czasie działania systemu.

Obsługa techniczna w trakcie pracy systemu zależy od pakietu jednostki systemowej. W pakiecie początkowym systemu (9402) nie ma możliwości korzystania z obsługi w trakcie pracy systemu. W zabezpieczeniu przez zapis lustrzany możliwa jest obsługa w trakcie pracy systemu tylko wtedy, kiedy sprzęt i zestaw systemu dysponuje tą obsługą. Najlepszą konfiguracją sprzętu z zabezpieczeniem przez zapis lustrzany jest ta, która gwarantuje maksymalny zakres obsługi w trakcie pracy systemu.

Istnieje wiele uszkodzeń, które mogą być pomyślnie usuwane w czasie normalnego działania systemu. Na przykład uszkodzenie głowicy napędu dysku nie spowoduje przerwania działania systemu. Jej wymiana i synchronizacja jednostki lustrzanej może być wykonywana w czasie działania systemu. Im wyższy jest poziom ochrony, tym częstsza jest możliwość korzystania z obsługi w trakcie pracy systemu.

W przypadku niektórych modeli system ogranicza poziom zabezpieczenia jednostki 1 i odpowiadającej jej jednostki lustrzanej do poziomu kontrolera. Rozdział ″Zabezpieczenie przez zapis lustrzany - reguły konfigurowania″ w książce Składowanie i odtwarzanie  zawiera więcej informacji na ten temat.

W niektórych warunkach do diagnozy uszkodzenia i jego naprawy konieczne jest wstrzymanie działania zabezpieczenia przez zapis lustrzany. Można wówczas wyłączyć system, aby ograniczyć czas jego działania bez zabezpieczenia przez zapis lustrzany. Niektóre naprawy muszą być przeprowadzane przy wyłączonym systemie. ***Obsługa odroczona*** oznacza czekanie z naprawą lub wymianą uszkodzonych elementów sprzętu związanych z dyskami do momentu, gdy będzie możliwe wyłączenie systemu. System jest dostępny, chociaż zabezpieczenie przez zapis lustrzany jest ograniczone z powodu uszkodzenia elementu sprzętu. Obsługa odroczona jest możliwa tylko w przypadku zabezpieczenia przez zapis lustrzany lub sprzętowego zabezpieczenia przez kontrolę parzystości.

***Para lustrzana:*** Dwie jednostki pamięci, które zawierają te same dane i są traktowane przez system jak jedna jednostka. ***Jednostka lustrzana*** jest jednostką pamięci należącą do pary lustrzanej.

***Jednostka dyskowa:*** Jest urządzeniem, które zawiera jednostki pamięci. Sprzęt zamawia się na poziomie jednostek dyskowych. Każda jednostka dyskowa ma własny numer seryjny.

***Jednostka pamięci:*** Jest obszarem adresowanym przez system, zdefiniowanym wewnątrz jednostki dyskowej.

***Jednostka:*** Jest zdefiniowanym fragmentem pamięci jednopoziomowej. Ten obszar jest najmniejszym adresowalnym przez użytkownika obszarem pamięci. Pula dyskowa stanowi jedną lub kilka jednostek identyfikowanych na podstawie unikalnego numeru jednostki. Jednostka w puli dyskowej bez zabezpieczenia przez zapis lustrzany stanowi jedną jednostkę pamięci. Jednostka w puli dyskowej z zabezpieczeniem przez zapis lustrzany tworzy parę lustrzaną, co oznacza, że są to dwie jednostki pamięci.

Za pomocą niektórych komend tworzenia (CRTPF, CRTJRNRCV itp.) można utworzyć obiekty na określonych jednostkach. W środowisku bez zabezpieczenia przez zapis lustrzany obiekty tworzone są na pojedynczych jednostkach pamięci. W środowisku z zabezpieczeniem przez zapis lustrzany wartość parametru UNIT oznacza parę lustrzaną.

Szczegóły dotyczące adresowania pamięci w serwerze zawiera sekcja Jak system adresuje pamięć.

***Wieża:*** Jest to zawierająca jednostki pamięci obudowa, którą system adresuje osobno.

***Magistrala:*** Jest głównym kanałem przesyłania danych wejściowych i wyjściowych. System może mieć więcej niż jedną magistralę.

***Procesor wejścia/wyjścia (IOP):*** Procesor wejścia/wyjścia (IOP) jest przyłączony do magistrali. IOP jest używany do przekazywania informacji pomiędzy pamięcią główną i określonymi grupami kontrolerów. Niektóre IOP są przeznaczone dla określonych typów kontrolerów, takich jak kontrolery dysków. Do innych IOP można przyłączyć kilka rodzajów kontrolerów, na przykład kontrolery napędów taśm i dysków.

***Adapter we/wy:*** Adapter we/wy (IOA) jest podłączony do procesora we/wy (IOP). Adapter we/wy przesyła dane pomiędzy procesorem IOP a jednostkami dyskowymi.

***Kontroler:*** Jest podłączony do procesora IOP i zajmuje się przekazywaniem informacji pomiędzy IOP a jednostkami dyskowymi. Niektóre jednostki dyskowe mają wbudowane kontrolery. Inne wymagają osobnych kontrolerów.

## Określanie, które pule dyskowe mają być chronione

Zabezpieczenie przez zapis lustrzany jest konfigurowane dla puli dyskowej, ponieważ jest to poziom użytkownika sterowania jednopoziomową pamięcią. Zabezpieczenia przez zapis lustrzany można używać do ochrony jednego, kilku lub wszystkich pul dyskowych w systemie. Jednak zabezpieczenie to nie wymaga utworzenia wielu pul dyskowych. Zabezpieczenie przez zapis lustrzany działa dobrze również wtedy, gdy wszystkie jednostki dyskowe w systemie są skonfigurowane w jednej puli dyskowej (domyślnie w serwerze iSeries). W rzeczywistości zapis lustrzany redukuje potrzebę partycjonowania pamięci dyskowej na pule dyskowe w celu ochrony i odtwarzania danych. Jednakże pule dyskowe mogą nadal być pożądane ze względu na ich wydajność, a także z innych powodów.

Aby zapewnić jak najlepszą ochronę i dostępność całego systemu, wszystkie pule dyskowe w systemie powinny mieć zabezpieczenie przez zapis lustrzany:

- Jeśli w systemie niektóre pule dyskowe mają zabezpieczenie przez zapis lustrzany, a niektóre nie, awaria jednostki dyskowej w puli dyskowej bez zabezpieczenia przez zapis lustrzany często ogranicza działanie całego systemu. Dane w puli dyskowej, w której wystąpiła awaria, mogą ulec utracie. Konieczne może się okazać ich długie odzyskiwanie.
- Jeśli awaria dysku wystąpi w puli dyskowej zabezpieczonej przez zapis lustrzany, a system zawiera również pule, które nie są zabezpieczone, dane nie ulegają utracie. Jednak w niektórych przypadkach niemożliwa jest w trakcie pracy systemu obsługa techniczna.

Jednostki dyskowe używane w pulach dyskowych powinny być starannie wybierane. Aby uzyskać najlepsze zabezpieczenie i wydajność, pula dyskowa powinna zawierać jednostki dyskowe podłączone do kilku różnych procesorów we/wy. Liczba jednostek dyskowych w puli dyskowej podłączonych do każdego procesora we/wy powinna być taka sama.

## Określenie liczby potrzebnych jednostek dyskowych

Pula dyskowa zabezpieczona przez zapis lustrzany wymaga podwójnej ilości pamięci, w porównaniu z pulą dyskową, która nie ma zabezpieczenia, ponieważ system zachowuje dwie kopie wszystkich danych w puli dyskowej. Przy zabezpieczeniu przez zapis lustrzany liczba jednostek dyskowych musi być parzysta, a jednostki muszą mieć jednakowe pojemności, aby można było utworzyć z nich pary lustrzane. Należy zauważyć, że w celu uzyskania wymaganej dodatkowej pojemności pamięci w istniejących systemach nie jest konieczne dodawanie takich samych jednostek dyskowych jak te, które są już dołączone. Dodane mogą

być dowolne nowe jednostki dyskowe, o ile zapewniona jest wystarczająca ilość pamięci i liczba jednostek o danej wielkości jest parzysta. System utworzy pary lustrzane i automatycznie przeniesie potrzebne dane. Jeśli pula dyskowa nie zawiera wystarczającej pamięci lub jeśli jednostki pamięci nie mogą być łączone w pary, nie można dla niej uruchomić zabezpieczenia przez zapis lustrzany.

Niezależnie od tego, czy system jest nowy, czy już istnieje, proces określania, jakie jednostki dyskowe są potrzebne do zabezpieczenia przez zapis lustrzany, jest podobny. Użytkownik i przedstawiciel handlowy IBM powinni:

1. Zaplanować ilość danych, jaką będzie zawierać każda pula dyskowa.
2. Zaplanować docelowy procent pamięci używanej w puli dyskowej (jak bardzo zapełniona będzie pula dyskowa).
3. Zaplanować liczbę i typ jednostek dyskowych potrzebnych do uzyskania wymaganej ilości pamięci. Dla istniejącej puli dyskowej, aby zapewnić wymaganą pamięć, można zaplanować inny typ i model jednostki dyskowej. Należy pamiętać, że liczba jednostek każdego typu i modelu powinna być parzysta.

Po zaplanowaniu wszystkich pul dyskowych należy podjąć decyzję o zaplanowanych jednostkach.

Po zebraniu wszystkich informacji można obliczyć łączną potrzebną pamięć.

***Planowanie pojemności pamięci:*** W przypadku nowego systemu przedstawiciel handlowy IBM może pomóc w analizie wymagań dotyczących pamięci. W przypadku istniejącego systemu bieżąca ilość danych w puli dyskowej, która jest planowana, stanowi odpowiedni punkt wyjścia. Opcja DST lub SST Wyświetlenie pojemności konfiguracji dysku określa łączną wielkość (w milionach bajtów) oraz procent pamięci użytej dla każdej puli dyskowej w systemie. Wielkość pul dyskowych należy pomnożyć przez procent używany do obliczania liczby megabajtów danych znajdujących się w puli dyskowej. W planowaniu przyszłych wymagań dotyczących pamięci dla puli dyskowej należy wziąć pod uwagę również wzrost systemu i jego wydajność.

Planowana ilość danych i planowany procent używanej pamięci określają łącznie ilość bieżącej pamięci dyskowej potrzebnej dla puli dyskowej z zabezpieczeniem przez zapis lustrzany. Na przykład, jeśli pula dyskowa ma zawierać 1 GB (GB jest równy 1 073 741 824 bajtów) bieżących danych, wymaga 2 GB pamięci na lustrzane kopie danych. Jeśli planowane jest 50% zapełnienie, pula dyskowa wymaga 4 GB bieżącej pamięci. Jeśli planowany procent ma wynosić 66%, konieczne jest 3 GB pamięci. Jeden gigabajt rzeczywistych danych (2 GB danych lustrzanych) w 5 GB puli dyskowej powoduje wykorzystanie pamięci dyskowej w 40%.

***Planowanie rezerwowych jednostek dyskowych:*** Rezerwowe jednostki dyskowe mogą ograniczyć czas, w którym system będzie działał bez zabezpieczenia przez zapis lustrzany po awarii jednostki dyskowej. W razie awarii rezerwa może zostać użyta do wymiany uszkodzonej jednostki pamięci. Za pomocą DST lub SST użytkownik może wybrać opcję wymiany uszkodzonej jednostki dyskowej na jednostkę rezerwową. System logicznie zastępuje uszkodzoną jednostkę wybraną jednostką rezerwową, a następnie synchronizuje nową jednostkę z pozostałą po awarii jednostką z pary lustrzanej. Po zakończeniu synchronizacji (zwykle po mniej niż godzinie) zabezpieczenie przez zapis lustrzany dla pary jest ponownie aktywne. Czas potrzebny na wymianę lub naprawę wadliwej jednostki może być o wiele dłuższy. Może upłynąć kilka godzin, które są potrzebne na powiadomienie serwisu i przeprowadzenie synchronizacji.

Aby w pełni wykorzystać zalety posiadania jednostek rezerwowych, należy zainstalować co najmniej po jednej takiej jednostce dla każdej pojemności jednostki w systemie. W ten sposób dla każdej wielkości jednostki dyskowej zostanie zapewniona rezerwa. Uszkodzoną jednostkę należy zastąpić jednostką o tej samej pojemności.

***Suma całkowitej potrzebnej pamięci:*** Po zaplanowaniu liczby i typu jednostek pamięci dla każdej puli dyskowej w systemie i dla wszystkich pozostałych jednostek pamięci należy dodać jednostki pamięci każdego typu i modelu. Należy pamiętać, że zaplanowana liczba dotyczy każdego typu jednostek, a nie wszystkich jednostek dyskowych. Użytkownik i przedstawiciel handlowy IBM przed zamówieniem sprzętu będą musieli na podstawie liczby zaplanowanych jednostek pamięci wyliczyć liczbę potrzebnych jednostek dyskowych.

Ta procedura służy do określenia całkowitej liczby jednostek dyskowych potrzebnych w systemie. Jeśli planuje się zainstalowanie nowego systemu, określona wartość jest liczbą jednostek, które trzeba zamówić. Jeśli planuje się zabezpieczenie przez zapis lustrzany dla istniejącego systemu, od uzyskanej wartości należy odjąć jednostki dyskowe, które są już w systemie. Tę liczbę nowych jednostek dyskowych należy zamówić.

## Określanie wymaganego poziomu zabezpieczenia

Poziom zabezpieczenia przez zapis lustrzany określa, kiedy system działa nadal w przypadku awarii różnych poziomów sprzętu. Poziom zabezpieczenia jest liczbą elementów sprzętu związanego z dyskami, mających swe kopie lustrzane. Im więcej jest par lustrzanych, które mają wyższy poziom zabezpieczenia, tym częściej system będzie działał w przypadku uszkodzenia sprzętu związanego z dyskami. Czasami można dojść do wniosku, że dla danego systemu niższy poziom zabezpieczenia jest bardziej uzasadniony ekonomicznie. Oto sześć poziomów zabezpieczenia przez zapis lustrzany, w kolejności od najniższego do najwyższego:

- Zabezpieczenie na poziomie jednostek dyskowych
- Zabezpieczenie na poziomie adaptera we/wy
- Zabezpieczenie na poziomie procesorów wejścia/wyjścia
- Zabezpieczenie na poziomie magistral
- Zabezpieczenie na poziomie wieży
- Zabezpieczenie na poziomie pierścienia

Przy podejmowaniu decyzji o poziomie zabezpieczenia powinno się wziąć pod uwagę relatywne korzyści każdej możliwości, mając na uwadze:

- Możliwość utrzymania działania systemu w czasie awarii sprzętu związanego z dyskami.
- Możliwość dokonania naprawy w trakcie pracy systemu. Aby zminimalizować czas, w którym para lustrzana jest niezabezpieczona, należy stworzyć możliwość naprawy uszkodzenia w czasie działania systemu.

W czasie operacji uruchamiania zabezpieczenia przez zapis lustrzany system tworzy pary jednostek dyskowych w taki sposób, aby zapewnić maksymalny poziom zabezpieczenia systemu. Po dodaniu jednostek dyskowych do lustrzanej puli dyskowej system łączy w pary tylko te jednostki dyskowe, które zostały dodane, nie zmienia zaś istniejących par. Konfiguracja sprzętu obejmuje sprzęt oraz sposób łączenia jego elementów.

Dalsze informacje dotyczące poziomów zabezpieczenia zawiera sekcja Poziomy zabezpieczenia – dalsze szczegóły.

***Poziomy zabezpieczenia – dalsze szczegóły:*** Poziom zabezpieczenia przez zapis lustrzany określa, kiedy system działa nadal w przypadku awarii różnych poziomów sprzętu. Zabezpieczenie przez zapis lustrzany zawsze zapewnia bezpieczeństwo na poziomie jednostki dyskowej, co wystarcza do utrzymania dostępności systemu w przypadku awarii pojedynczej jednostki dyskowej. Aby system pozostawał dostępny w przypadku uszkodzeń innych elementów sprzętu dyskowego, konieczny jest wyższy poziom zabezpieczenia. Jeśli system ma pozostać dostępny, na przykład w sytuacji uszkodzenia procesora wejścia/wyjścia (IOP), wszystkie jednostki dyskowe, które podłączone są do tego procesora, muszą mieć lustrzane jednostki podłączone do innego IOP.

Poziom zabezpieczenia przez zapis lustrzany decyduje także o tym, czy w wypadku rozmaitych typów awarii jest możliwa obsługa techniczna w trakcie pracy systemu. W przypadku pewnych typów uszkodzeń obsługa w trakcie pracy systemu jest niezbędna do diagnozowania poziomów sprzętu powyżej elementu, który uległ awarii. Na przykład diagnozowanie zasilania jednostki dyskowej, procesora I/O, do którego podłączona jest uszkodzona jednostka, wymaga zresetowania. Z tego powodu wymagane jest zabezpieczenie na poziomie IOP. Im wyższy jest poziom zabezpieczenia, tym częstsza jest możliwość obsługi w trakcie pracy systemu.

Poziom zabezpieczenia zależy od duplikowanego sprzętu. Jeśli duplikuje się jednostki dyskowe, zabezpieczenie jest na poziomie jednostek dyskowych. Jeśli duplikowane są również kontrolery jednostek dyskowych, zabezpieczenie jest na poziomie kontrolerów. Jeśli zaś duplikowane są procesory I/O,

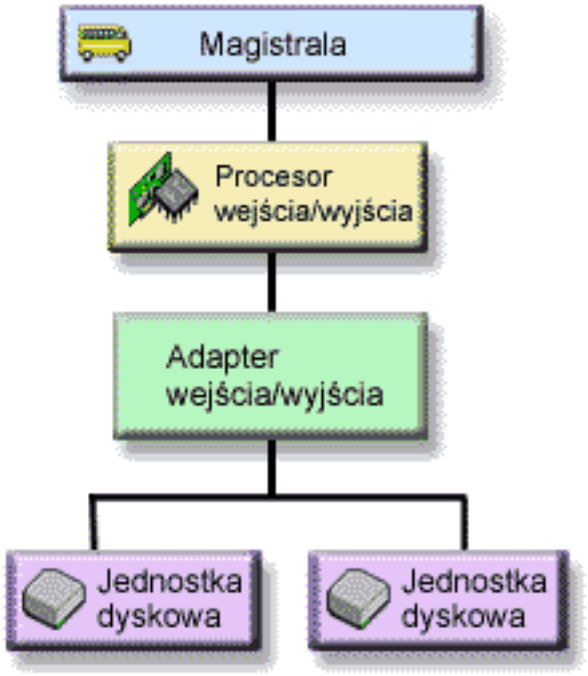
zabezpieczenie jest na poziomie IOP. Podczas gdy duplikowane są magistrale, zabezpieczenie jest na poziomie magistral. Jednostki lustrzane mają zabezpieczenie na poziomie co najmniej jednostek dyskowych. Większość jednostek dyskowych ma wbudowane kontrolery, dlatego zwykle są one zabezpieczone na poziomie kontrolerów.

W czasie operacji uruchamiania zabezpieczenia przez zapis lustrzany system tworzy pary jednostek dyskowych w taki sposób, aby zapewnić maksymalny poziom zabezpieczenia systemu. Po dodaniu jednostek dyskowych do lustrzanej puli dyskowej system łączy w pary tylko te jednostki dyskowe, które zostały dodane, nie zmienia zaś istniejących par. Konfiguracja sprzętu obejmuje sprzęt oraz sposób łączenia jego elementów.

***Zabezpieczenie na poziomie jednostek dyskowych:*** Zabezpieczenie przez zapis lustrzany zawsze zapewnia zabezpieczenie na poziomie jednostki dyskowej, ponieważ jednostki pamięci są duplikowane. Jeśli nacisk kładzie się na bezpieczeństwo danych, a nie na ich wysoką dostępność, zabezpieczenie na poziomie jednostki dyskowej może być wystarczające. Jednostka dyskowa jest elementem, który najszybciej może zawieść, a zabezpieczenie na poziomie jednostki dyskowej wystarcza do zapewnienia dostępności systemu po wystąpieniu awarii jednostki dyskowej.

Przy zabezpieczeniu na poziomie jednostek dyskowych, w przypadku niektórych typów awarii jednostek dyskowych możliwa jest obsługa techniczna w trakcie pracy systemu.

Poniższy rysunek przedstawia elementy zabezpieczenia na poziomie jednostki dyskowej: jedną magistralę podłączoną do jednego procesora IOP, który z kolei jest podłączony do jednego adaptera IOA podłączonego do dwóch oddzielnych jednostek dyskowych. Dwie jednostki pamięci tworzą parę lustrzaną. W przypadku tego zabezpieczenia system działa bez przerwy po uszkodzeniu jednostki dyskowej. Jeśli zawiedzie kontroler lub procesor I/O, system nie będzie mógł uzyskać dostępu do danych znajdujących się na żadnej z jednostek pary lustrzanej i nie będzie mógł być używany.



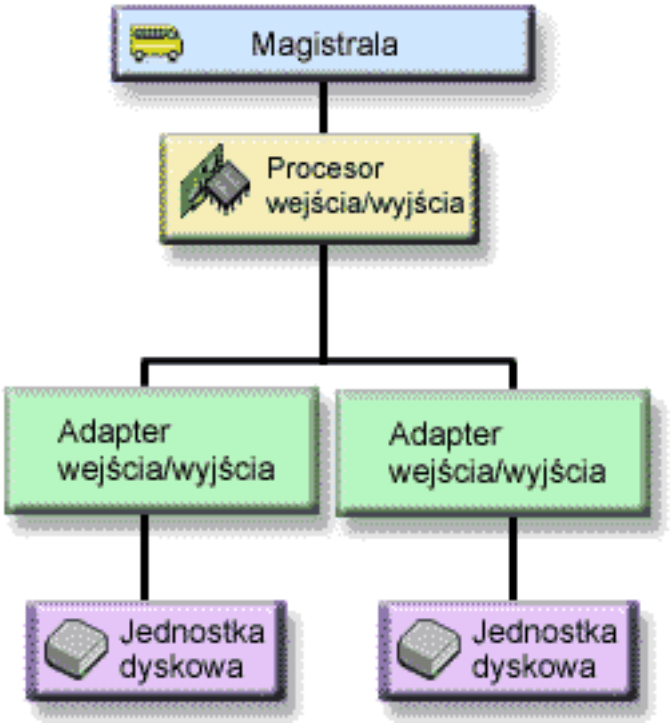

***Zabezpieczenie na poziomie adaptera we/wy:*** Należy określić, czy zabezpieczenie na poziomie adaptera we/wy ma:

- Zachować możliwość dostępu do systemu w przypadku awarii adaptera IOA.

- Umożliwić jednoczesną naprawę uszkodzonej jednostki dyskowej lub adaptera IOA. Aby użyć procedur rozwiązywania problemów podczas przygotowania do wyodrębnienia uszkodzonej pozycji lub do sprawdzenia wyniku naprawy, adapter IOA musi być wyznaczony do naprawy. Jeśli jakieś jednostki dyskowe podłączone do adaptera IOA nie mają zabezpieczenia na poziomie adaptera IOA, ta część współbieżnej konserwacji nie jest możliwa.

Aby uzyskać zabezpieczenie na poziomie adaptera IOA, wszystkie jednostki dyskowe muszą mieć lustrzaną jednostkę podłączoną do innego adaptera IOA. Ten rysunek przedstawia zabezpieczenie na poziomie adaptera IOA. Dwie jednostki pamięci tworzą parę lustrzaną. W przypadku zabezpieczenia na poziomie adaptera IOA system może kontynuować działanie w przypadku awarii adaptera IOA. Jeśli zawiedzie procesor I/O, system nie będzie mógł uzyskać dostępu do danych znajdujących się na jednostkach pary lustrzanej i nie będzie mógł być używany.

Rysunek przedstawia elementy zabezpieczenia na poziomie adaptera IOA: jedną magistralę podłączoną do jednego procesora IOP, podłączonego z kolei do dwóch adapterów IOA, z których każdy łączy się z dwoma oddzielnymi jednostkami dyskowymi.

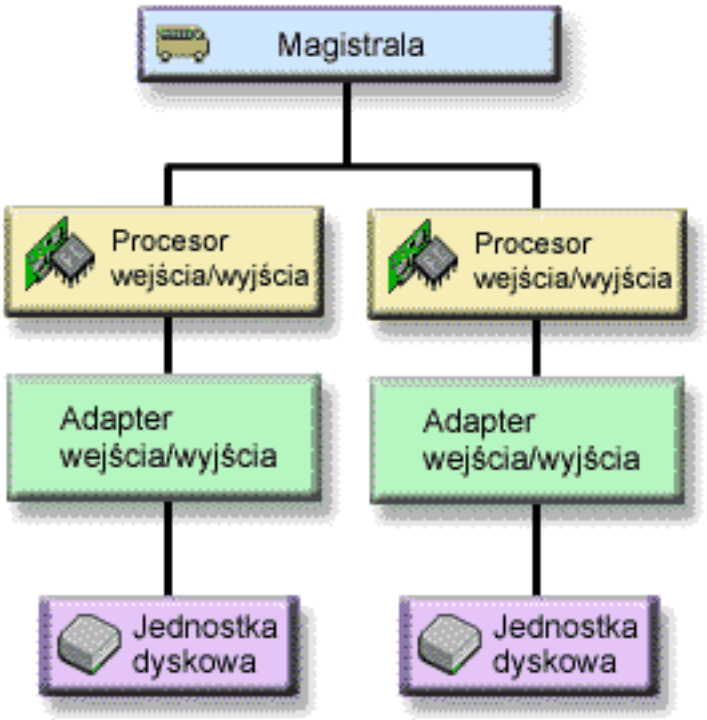



***Zabezpieczenie na poziomie procesorów wejścia/wyjścia:*** Aby określić, czy zabezpieczenie na poziomie IOP jest potrzebne, należy wziąć pod uwagę:

- Zachowanie dostępności systemu w przypadku uszkodzenia IOP.
- Zachowanie dostępności systemu w przypadku uszkodzenia kabla podłączonego do IOP.
- Naprawę pewnych typów uszkodzeń jednostki dyskowej lub kabla bez wyłączania systemu. Uszkodzenia tych typów powodują, że obsługa techniczna w trakcie pracy systemu wymaga zresetowania procesora IOP. Jeśli jakaś jednostka dyskowa, która została podłączona do IOP, nie jest zabezpieczona na poziomie IOP, wówczas obsługa w trakcie pracy systemu nie jest możliwa.

Aby uzyskać zabezpieczenie na poziomie IOP, wszystkie jednostki dyskowe muszą mieć jednostki lustrzane podłączone do innego IOP. W wielu systemach zabezpieczenie na poziomie procesorów wejścia/wyjścia nie jest możliwe w przypadku pary lustrzanej zawierającej jednostkę 1.

Poniższy rysunek przedstawia elementy zabezpieczenia na poziomie adaptera IOP: jedną magistralę, podłączoną do dwóch procesorów IOP, które są z kolei podłączone do dwóch oddzielnych adapterów IOA i dwóch oddzielnych jednostek dyskowych. Dwie jednostki pamięci tworzą parę lustrzaną. W przypadku zabezpieczenia na poziomie procesora IOP system może kontynuować działanie w przypadku awarii jednego procesora we/wy. Systemu nie można używać tylko w przypadku awarii magistrali.

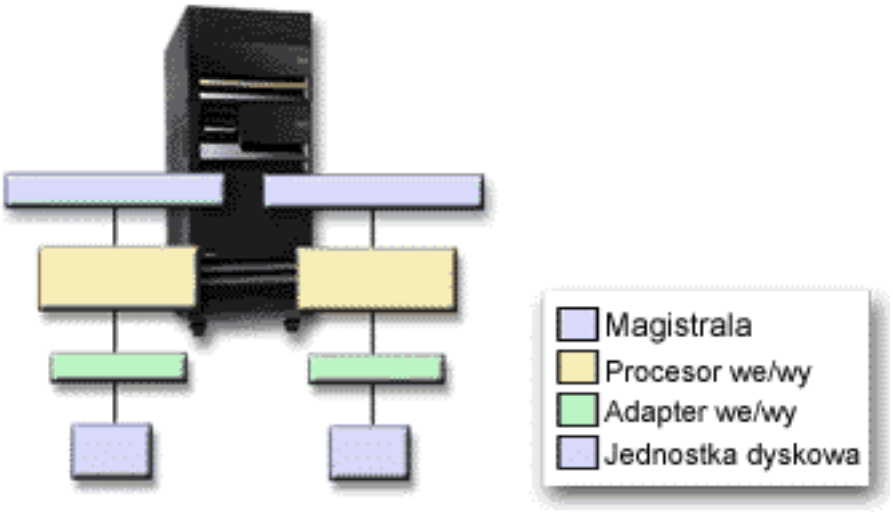



***Zabezpieczenie na poziomie magistrali:*** Zabezpieczenie na poziomie magistrali gwarantuje działanie systemu po uszkodzeniu magistrali. Jednak zabezpieczenie takie często jest nieopłacalne, ponieważ:

- System nie będzie mógł działać w przypadku uszkodzenia magistrali 1.
- Jeśli zawiedzie magistrala, operacje wejścia/wyjścia dysku mogą być kontynuowane, ale większość pozostałego sprzętu nie działa (na przykład stacje robocze, drukarki i linie komunikacyjne) i dlatego system praktycznie jest niedostępny.
- Awarie magistrali są rzadkie w porównaniu do uszkodzeń innych elementów sprzętu dyskowego.
- W przypadku awarii magistrali niemożliwa jest obsługa techniczna w trakcie pracy systemu.

Aby uzyskać zabezpieczenie na poziomie magistrali, wszystkie jednostki dyskowe muszą mieć jednostki lustrzane podłączone do innej magistrali. W przypadku jednostki 1 zabezpieczenie na poziomie magistrali jest niemożliwe.

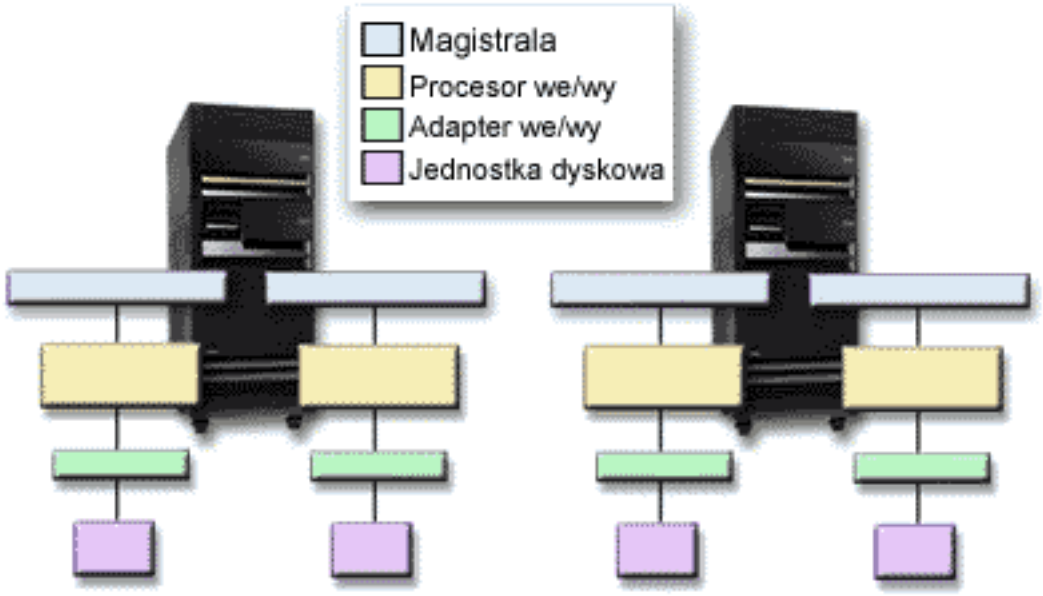
Rysunek przedstawia elementy zabezpieczenia na poziomie magistrali: jedną wieżę zawierającą dwie magistrale podłączone do oddzielnych procesorów IOP, adapterów IOA i jednostek dyskowych. Dwie jednostki pamięci tworzą parę lustrzaną. W tym przypadku system może działać bez przerwy po uszkodzeniu magistrali. System nie będzie mógł jednak działać w przypadku uszkodzenia magistrali 1.




***Zabezpieczenie na poziomie wieży:*** Zabezpieczenie na poziomie wieży umożliwia uruchomienie systemu po uszkodzeniu wieży. Jednak zabezpieczenie takie często jest nieopłacalne, ponieważ:

- Jeśli zawiedzie wieża, operacje wejścia/wyjścia dysku mogą być kontynuowane, ale większość pozostałego sprzętu nie działa (na przykład stacje robocze, drukarki i linie komunikacyjne), a więc system jest praktycznie niedostępny.
- Awarie wieży są rzadkie w porównaniu do uszkodzeń innych elementów sprzętu dyskowego.

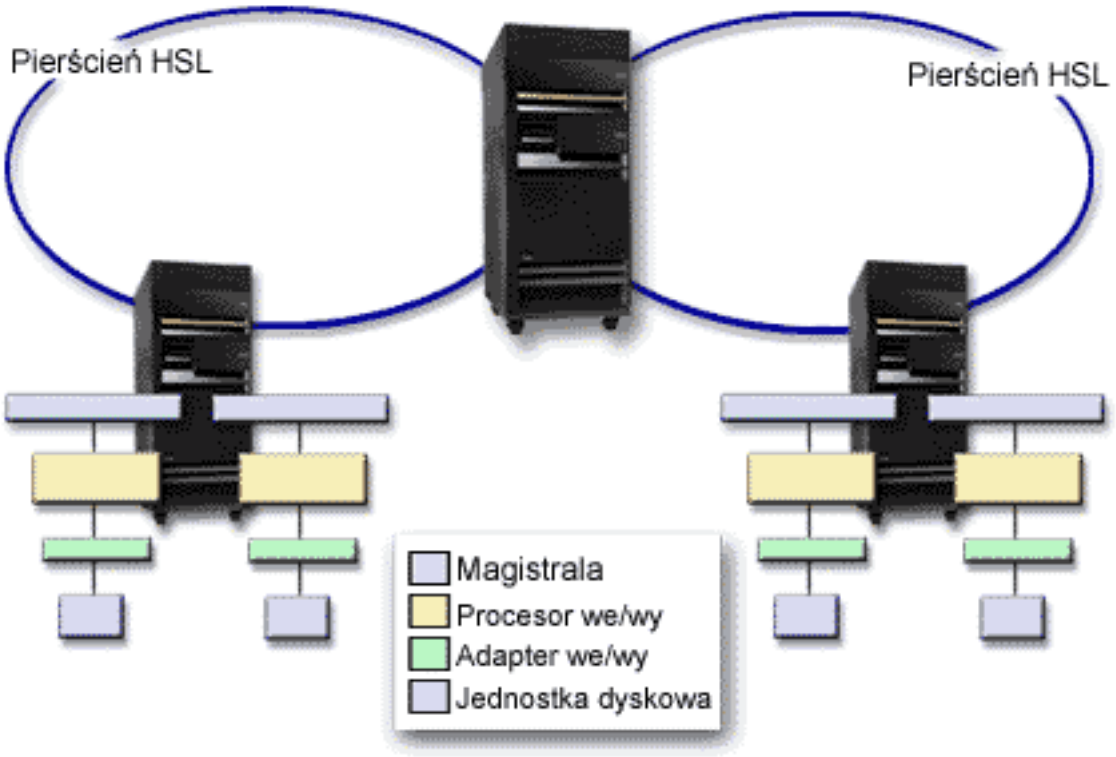
Aby uzyskać zabezpieczenie na poziomie wieży, wszystkie jednostki dyskowe podłączone do danej wieży, muszą mieć jednostki lustrzane podłączone do innej wieży. Rysunek przedstawia elementy zabezpieczenia na poziomie wieży: dwie wieże, z których każda zawiera dwie magistrale, które są podłączone do oddzielnych procesorów IOP, adapterów IOA i jednostek dyskowych.



***Zabezpieczenie na poziomie pierścienia:*** Zabezpieczenie na poziomie pierścienia umożliwia uruchomienie systemu po uszkodzeniu łącza o dużej szybkości (HSL). Jednak zabezpieczenie takie często jest nieopłacalne, ponieważ:

- Jeśli łącze HSL zostanie uszkodzone, operacje wejścia/wyjścia dysku mogą być kontynuowane, ale większość pozostałego sprzętu nie działa (na przykład stacje robocze, drukarki i linie komunikacyjne), a więc system jest praktycznie niedostępny.
- Awarie łącza HSL są rzadkie w porównaniu do uszkodzeń innych elementów sprzętu dyskowego.

Aby uzyskać zabezpieczenie na poziomie pierścienia, wszystkie jednostki dyskowe podłączone do wieży w jednym HSL muszą mieć jednostki lustrzane podłączone do innej wieży w innym HSL. Rysunek przedstawia elementy zabezpieczenia na poziomie pierścienia: dwa pierścienie HSL podłączone do dwóch wież, z których każda zawiera dwie magistrale, które są podłączone do oddzielnych procesorów IOP, adapterów IOA i jednostek dyskowych.




## Określanie sprzętu potrzebnego do zabezpieczenia przez zapis lustrzany

Aby jednostki dyskowe mogły komunikować się z resztą systemu, podłączone są do kontrolerów, które z kolei podłączone są do procesorów I/O, a te do magistral. Liczba tych elementów sprzętu związanego z dyskami dostępna w systemie ma wpływ na możliwy do uzyskania poziom zabezpieczenia.

Aby uzyskać najlepsze zabezpieczenie i wydajność, każdy poziom sprzętu powinien być dopasowany do następnego poziomu. Z tego powodu liczba jednostek dyskowych każdego typu i modelu, które są podłączone do kontrolerów, powinna być parzysta. Do każdego procesora powinna być podłączona ta sama liczba kontrolerów każdego typu dysków. Liczba IOP powinna być dostosowana do dostępnych magistral.

Aby zaplanować, jaki sprzęt dyskowy jest potrzebny do zabezpieczenia przez zapis lustrzany danego systemu, należy określić całkowitą liczbę i typ jednostek dyskowych (starych i nowych), które będą potrzebne w systemie, oraz poziom zabezpieczenia systemu. Nie zawsze można tak skonfigurować system,

aby wszystkie pary lustrzane spełniały zakładany poziom zabezpieczenia. Można jednak zaplanować taką konfigurację, w której większość jednostek dyskowych spełni założenia dotyczące poziomu zabezpieczenia systemu.

Podczas planowania dodatkowego sprzętu związanego z dyskami należy wykonać następujące czynności:

1. Określić minimalną ilość sprzętu niezbędnego do funkcjonowania zaplanowanych jednostek dyskowych. Nie powinno się równocześnie planować zabezpieczeń dla jednostek dyskowych różnej wielkości.
2. Zaplanować dodatkowy sprzęt potrzebny do zapewnienia potrzebnego poziomu zabezpieczenia dla wszystkich typów jednostek dyskowych.

***Planowanie minimum sprzętu niezbędnego do działania:*** Przy łączeniu ze sobą sprzętu związanego z dyskami obowiązują różne reguły i ograniczenia. Ograniczenia mogą wynikać z budowy sprzętu, architektury czy założeń dotyczących wydajności lub obsługi. Przedstawiciel handlowy IBM może wyjaśnić te limity konfiguracji i pomóc w ich uwzględnianiu podczas planowania. Aby uzyskać listę ograniczeń i reguł konfiguracji, należy przejrzeć temat Instalowanie, aktualizacja i migracja.

Dla każdego typu jednostki dyskowej należy najpierw zaplanować instalację odpowiednich kontrolerów, a następnie IOP. Po określeniu liczby IOP dla każdego typu dysku należy wykorzystać całkowitą liczbę procesorów do zaplanowania liczby magistral, które będą potrzebne.

***Planowanie dodatkowego sprzętu niezbędnego dla wybranego poziomu zabezpieczenia:***

- Zabezpieczenie na poziomie jednostek dyskowych
  Jeśli zaplanowano zabezpieczenie na poziomie jednostek dyskowych, nie trzeba wykonywać żadnych dodatkowych czynności. Wszystkie pule dyskowe z zabezpieczeniem przez zapis lustrzany mają minimalne zabezpieczenie na poziomie jednostki dyskowej, jeśli spełniają wymagania dotyczące uruchamiania zabezpieczenia przez zapis lustrzany.
- Zabezpieczenie na poziomie kontrolerów
  Jeśli zaplanowane jednostki dyskowe nie wymagają oddzielnego kontrolera, zabezpieczenie na poziomie kontrolera zostało już osiągnięte i nie trzeba wykonywać żadnych czynności. Jeśli zaplanowane jednostki dyskowe wymagają oddzielnego kontrolera, należy dodać tyle kontrolerów, na ile pozwalają ograniczenia systemu. Następnie, zgodnie z zasadami konfiguracji, należy odpowiednio rozłożyć jednostki dyskowe.
- Zabezpieczenie na poziomie procesorów wejścia/wyjścia
  Jeśli w systemie ma zostać zastosowane zabezpieczenie na poziomie IOP i nie ma jeszcze maksymalnej liczby procesorów, należy dodać ich tyle, na ile pozwalają ograniczenia systemu. Następnie, zgodnie z zasadami konfiguracji, należy odpowiednio rozłożyć jednostki dyskowe. Aby podłączyć więcej IOP, należy dołączyć dodatkowe magistrale.
- Zabezpieczenie na poziomie magistral
  Jeśli system ma wiele magistral i ma być zabezpieczony na poziomie magistrali, nie trzeba wykonywać żadnych czynności. Jeśli system został skonfigurowany zgodnie ze standardowymi zasadami, funkcja zabezpieczania przez zapis lustrzany łączy w pary możliwie największą liczbę jednostek dyskowych. Jeśli system ma jedną magistralę, można dodać dodatkową magistralę jako opcjonalną.
- Zabezpieczenie na poziomie wieży
  Jeśli system jest skonfigurowany w ten sposób, że w różnych wieżach jest jednakowa liczba jednostek dyskowych o jednakowych pojemnościach, funkcja łącząca w pary kopie lustrzane sparuje jednostki dyskowe znajdujące się w różnych wieżach w celu zapewnienia zabezpieczenia na poziomie wieży na tylu jednostkach dyskowych, na ilu jest to możliwe.
- Zabezpieczenie na poziomie pierścienia
  Jeśli system jest skonfigurowany w ten sposób, że w różnych łączach o dużej szybkości (HSL) jest jednakowa liczba jednostek dyskowych o jednakowych pojemnościach, funkcja łącząca w pary kopie lustrzane sparuje jednostki dyskowe znajdujące się w różnych łączach o dużej szybkości (HSL) w celu zapewnienia zabezpieczenia na poziomie pierścienia na tylu jednostkach dyskowych, na ilu jest to możliwe.

## Określanie dodatkowego sprzętu niezbędnego do zapewnienia wymaganej wydajności

Zwykle zabezpieczenie przez zapis lustrzany wymaga zainstalowania dodatkowych jednostek dyskowych i procesorów wejścia/wyjścia. W pewnych przypadkach do zapewnienia wymaganej wydajności może być potrzebny dodatkowy sprzęt.

Poniższe informacje pomogą zdecydować, ile dodatkowego sprzętu należy zapewnić:

- **Wymagania dotyczące procesora**

  Zabezpieczenie przez zapis lustrzany powoduje znikomy wzrost wykorzystania CPU (w przybliżeniu od 1% do 2%).

- **Wymagania dotyczące pamięci głównej**

  Jeśli system ma zabezpieczenie przez zapis lustrzany, należy zwiększyć wielkość puli maszynowej. Zabezpieczenie przez zapis lustrzany wymaga pamięci w puli maszynowej do celów ogólnych oraz dla każdej pary lustrzanej. Każdy 1 GB pamięci na zabezpieczonym przez zapis lustrzany dysku wiąże się ze zwiększeniem wielkości puli pamięci maszyny o około 12 kB (12 kB dla 1 GB DASD, 24 kB dla 2 GB DASD itd.).

  W czasie synchronizacji zabezpieczenie przez zapis lustrzany korzysta z dodatkowych 512 kB pamięci dla każdej synchronizowanej pary lustrzanej. System używa puli, w której jest najwięcej pamięci.

- **Wymagania dotyczące procesorów IOP**

  Aby wydajność systemu była taka sama, jak przed uruchomieniem zabezpieczenia przez zapis lustrzany, w systemie powinien zostać zachowany taki sam stosunek liczby jednostek dyskowych do liczby IOP. Dodanie IOP może wiązać się z koniecznością instalacji dodatkowej magistrali.

  Ponieważ istnieją ograniczenia zwiększania liczby magistral i IOP, zachowanie stosunku jednostek dyskowych do IOP może okazać się niemożliwe. W tym przypadku wydajność systemu może być niższa.

Dodatkowe informacje o wpływie zapisu lustrzanego na wydajność zawiera sekcja Zapis lustrzany a wydajność.

***Zapis lustrzany a wydajność:*** Kiedy uruchamia się zabezpieczenie przez zapis lustrzany, w większości systemów obserwuje się niewielką zmianę wydajności; w niektórych przypadkach zabezpieczenie przez zapis lustrzany może spowodować wzrost wydajności. Przy zabezpieczeniu przez zapis lustrzany funkcje, które wykonują głównie operacje odczytu, generalnie realizowane są z taką samą lub lepszą wydajnością. Jest to spowodowane tym, że operacje odczytu mogą być wykonywane z dwóch jednostek pamięci, przy czym wybierana jest ta, która zapewnia krótszy czas dostępu. Przy zabezpieczeniu przez zapis lustrzany funkcje, które wykonują głównie operacje zapisu (na przykład aktualizacja rekordów baz danych), mogą być realizowane z niewiele gorszą wydajnością, ponieważ wszystkie zmiany muszą być zachowywane na obu jednostkach pamięci z pary lustrzanej. Z tego powodu operacje odtwarzania są wolniejsze.

W niektórych przypadkach, jeśli praca systemu zostanie przerwana, nie można określić, czy ostatni zapis został dokonany na obu jednostkach pamięci z pary lustrzanej. Kiedy system nie może tego ustalić, wykonywana jest synchronizacja pary lustrzanej. Polega to na tym, że dane z jednej jednostki kopiowane są na drugą jednostkę z pary lustrzanej. Synchronizacja występuje w czasie IPL po nienormalnym zakończeniu pracy systemu. Jeśli system może zachować kopię pamięci głównej przed zakończeniem pracy, proces synchronizacji zabiera tylko kilka minut. W przeciwnym wypadku proces synchronizacji trwa dużo dłużej. W sytuacji krańcowej może być przeprowadzana pełna synchronizacja.

Jeśli często zdarzają się wyłączenia zasilania, należy rozważyć zastosowanie zasilacza awaryjnego (UPS). W przypadku utraty zasilania UPS pozwala na kontynuację pracy systemu. Podstawowy zasilacz awaryjny pozwala na zachowanie pamięci głównej przed zakończeniem pracy systemu i uniknięcie długiego odzyskiwania. Obie jednostki dyskowe z pary lustrzanej źródła ładowania systemu muszą być zasilane przez UPS.

### Zamówienie nowego sprzętu
Przedstawiciel handlowy IBM pomoże podczas zamawiania nowego sprzętu w trybie normalnego procesu zamówienia. Proces ten umożliwia uwzględnienie wszystkich dodatkowych elementów potrzebnych podczas modernizacji (na przykład ramek czy kabli).

### Planowanie instalacji
Należy wspólnie z przedstawicielem handlowym IBM zaplanować instalację zabezpieczenia przez zapis lustrzany w systemie. Przedstawiciel handlowy pomoże w określeniu, czy system jest zrównoważony i spełnia standardowe reguły konfigurowania, zdefiniowane w publikacji Instalowanie, aktualizacje i migracja. System musi być skonfigurowany zgodnie ze standardowymi zasadami, aby funkcja grupowania w pary jednostek pamięci mogła zapewnić najlepszą możliwą ochronę w ramach dostępnego sprzętu. Przedstawiciel handlowy pomoże również w planowaniu nowych jednostek, które należy dodać do każdej puli dyskowej.

Jeśli zabezpieczenie przez zapis lustrzany ma zostać uruchomione w nowym systemie, to można być pewnym, że będzie on skonfigurowany zgodnie ze standardowymi zasadami konfiguracji. Jeśli używany jest starszy system, może on odbiegać od tych zasad. Zanim jednak zacznie się zmieniać konfigurację sprzętu, należy spróbować uruchomić zabezpieczenie przez zapis lustrzany.

Więcej informacji na temat sposobu planowania pul dyskowych zawiera sekcja Planowanie tworzenia pul dyskowych.

***Planowanie tworzenia pul dyskowych:*** Należy zaplanować pule dyskowe użytkowników, które będą zabezpieczone przez zapis lustrzany i określić, jakie jednostki dodać do pul dyskowych. Książka

Składowanie i odtwarzanie  zawiera informacje o sposobie przypisywania jednostek dyskowych dodawanych do pul dyskowych.

Jednostki w puli dyskowej należy równomiernie rozdzielić na kilka procesorów we/wy. Nie należy podłączać wszystkich jednostek do tego samego procesora we/wy. Zapewnia to lepsze zabezpieczenie i wydajność.

### Instalowanie nowego sprzętu
Dostarczany sprzęt jest instalowany przez przedstawiciela serwisu. Po zainstalowaniu sprzętu należy przejrzeć sekcję Dodanie jednostki dyskowej lub puli dyskowej, aby uzyskać informacje na temat sposobu dodawania nowych jednostek i uruchamiania zabezpieczenia przez zapis lustrzany.

## Zabezpieczenie przez zdalny zapis lustrzany DASD
Przy standardowej obsłudze zapisu lustrzanego DASD konieczne jest, aby obie jednostki dyskowe z pary źródła ładowania systemu (jednostka 1) były podłączone do procesora MFIOP. Zapewnia to możliwość przeprowadzenia IPL z jednego z dwóch źródeł pary lustrzanej lub zrzucenia na nią pamięci głównej w przypadku nienormalnego zakończenia działania systemu. Ponieważ jednak oba te źródła muszą być podłączone do tego samego IOP, najlepszym poziomem zabezpieczenia dla tej pary jest poziom kontrolera. Aby zwiększyć poziom zabezpieczenia systemu, można użyć zdalnego zapisu lustrzanego źródła ładowania systemu i zdalnego zapisu lustrzanego DASD.

Zabezpieczenie przez zdalny zapis lustrzany DASD w połączeniu ze zdalnym zapisem lustrzanym źródła ładowania systemu tworzy kopie lustrzane DASD, dołączone do lokalnych magistral optycznych, używając DASD dołączonych do magistral optycznych kończących się w miejscu zdalnym. W tej konfiguracji cały system, łącznie ze źródłem ładowania systemu, może być zabezpieczony. Jeśli uszkodzone zostanie miejsce zdalne, system może nadal działać na DASD znajdującym się w miejscu lokalnym. Jeśli lokalny DASD i jednostka systemowa są uszkodzone, nowa jednostka systemowa może zostać podłączona do zestawu DASD połączonych zdalnie. W ten sposób można przywrócić przetwarzanie systemu.

Zabezpieczanie przez zdalny zapis lustrzany DASD obsługuje umieszczanie jednostek dyskowych ze sprzętowym zabezpieczeniem przez kontrolę parzystości w tej samej puli dyskowej z jednostkami dyskowymi zabezpieczonymi przez zapis lustrzany; sprzętowe zabezpieczenie przez kontrolę parzystości

DASD może być aktywne w miejscu lokalnym lub zdalnym. Jednakże jeśli w miejscu katastrofy było aktywne sprzętowe zabezpieczenie przez kontrolę parzystości DASD, wszystkie dane w pulach dyskowych z takim zabezpieczeniem zostaną utracone.

Obsługa zdalnego zapisu lustrzanego umożliwia podzielenie jednostek dyskowych systemu na grupy lokalnych DASD i grupy zdalnych DASD. Zdalne DASD są podłączone do jednego zestawu magistral optycznych. Lokalne DASD podłączone są do innego zestawu. Lokalne i zdalne DASD mogą być fizycznie rozdzielone przez poprowadzenie odpowiednich magistral optycznych do zdalnego miejsca. Odległość między tymi miejscami jest ograniczona przez odległość, na jaką mogą zostać rozciągnięte magistrale optyczne.

Dalsze informacje opisujące zdalny zapis lustrzany DASD znajdują się w poniższych sekcjach:
- Zdalny zapis lustrzany DASD – zalety
- Zdalny zapis lustrzany DASD – wady
- Porównanie standardowego i zdalnego zabezpieczenia przez zapis lustrzany

Po wybraniu zdalnego zapisu lustrzanego DASD jako metody właściwej dla danego systemu należy przygotować system, a następnie rozpocząć zdalny zapis lustrzany.

## Zdalny zapis lustrzany źródła ładowania systemu

Zdalny zapis lustrzany źródła ładowania systemu umożliwia dołączenie dwóch jednostek dyskowych źródła ładowania systemu do dwóch różnych procesorów IOP lub dwóch magistral systemowych, co jednocześnie stanowi zabezpieczenie na poziomie procesorów wejścia/wyjścia lub magistrali. W takim jednak wypadku IPL może zostać wykonany tylko ze źródła ładowania systemu podłączonego do procesora MFIOP. Podobnie jest w przypadku zrzutu pamięci głównej. Jeśli uszkodzeniu ulegnie źródło ładowania systemu podłączone do procesora MFIOP, system będzie mógł kontynuować działanie z drugiego dysku z pary lustrzanej, ale nie będzie mógł wykonać IPL ani zrzutu pamięci głównej do czasu naprawy dysku podłączonego do procesora MFIOP.

Dalsze informacje opisujące zdalny zapis lustrzany źródła ładowania systemu zawierają poniższe sekcje:
- Włączenie zdalnego zapisu lustrzanego źródła ładowania systemu
- Wyłączenie zdalnego zapisu lustrzanego źródła ładowania systemu
- Użycie zdalnego zapisu lustrzanego źródła ładowania systemu z lokalnymi DASD

***Włączenie zdalnego zapisu lustrzanego źródła ładowania systemu:*** Aby obsłużyć zdalny zapis lustrzany dysku źródła ładowania systemu, zapis lustrzany musi najpierw zostać włączony. Zabezpieczenie przez zapis lustrzany należy uruchomić dla puli dyskowej 1. Jeśli zdalny zapis lustrzany źródła ładowania systemu został włączony po włączeniu zabezpieczenia przez zapis lustrzany dla puli dyskowej 1, istniejące zabezpieczenie przez zapis lustrzany i proces łączenia w pary lustrzanych źródeł ładowania nie ulegnie zmianie.

Zabezpieczenie przez zdalny zapis lustrzany źródła ładowania systemu można włączyć w środowisku DST lub SST w iSeries Navigator lub w interfejsie znakowym. Jeśli zdalny zapis lustrzany dysku źródła ładowania systemu jest już włączony, przy próbie jego włączenia wyświetli się komunikat informujący o tym, że zapis lustrzany został już włączony. Nie ma innych komunikatów o błędach lub ostrzeżeń przy włączeniu obsługi zdalnego zapisu lustrzanego źródła ładowania systemu.

Aby włączyć zdalny zapis lustrzany źródła ładowania systemu, wykonaj następujące czynności:
1. Z głównego menu DST wybierz opcję 4, Praca z jednostkami dyskowymi.
2. Z menu Praca z jednostkami dyskowymi (Work with Disk Units) wybierz opcję 1, Praca z konfiguracją dysków.
3. Z menu Praca z konfiguracją dysków (Work with Disk Configuration) wybierz opcję 4, Praca z zabezpieczeniem przez zapis lustrzany.

4. Z menu Praca z zabezpieczeniem przez zapis lustrzany (Work with Mirrored Protection) wybierz opcję 4, Włączenie zdalnego zapisu lustrzanego źródła ładowania systemu. Spowoduje to wyświetlenie ekranu potwierdzenia Włączenie zdalnego zapisu lustrzanego źródła ładowania systemu (Enable remote load source mirroring).
5. Na tym ekranie naciśnij klawisz Enter. U dołu ekranu Praca z zabezpieczeniem przez zapis lustrzany (Work with mirrored protection) wyświetlony zostanie komunikat o włączeniu zdalnego zapisu lustrzanego źródła ładowania systemu.

***Wyłączenie zdalnego zapisu lustrzanego źródła ładowania systemu:*** Aby wyłączyć obsługę zdalnego zapisu lustrzanego źródła ładowania systemu, należy:

- zatrzymać zabezpieczenie przez zapis lustrzany, a następnie wyłączyć obsługę zdalnego zapisu lustrzanego źródła ładowania systemu

lub

- przenieść zdalne źródło ładowania systemu do procesora MFIOP, a następnie wyłączyć obsługę zdalnego zapisu lustrzanego źródła ładowania systemu.

  Jeśli zdalne źródło ładowania systemu zostanie przeniesione do procesora MFIOP, IOP i system mogą go nie rozpoznać, ponieważ różne IOP mogą stosować różne wielkości formatów DASD. Jeśli po przeniesieniu do procesora MFIOP dane zdalnego źródła ładowania systemu zostaną utracone, należy użyć funkcji zamiany jednostek dyskowych DST do zastąpienia źródła ładowania systemu nim samym. Spowoduje to, że DASD zostanie ponownie sformatowany w taki sposób, aby procesor MFIOP mógł go użyć. Następnie jednostka dyskowa zostanie zsynchronizowana z aktywnym źródłem ładowania systemu.

Zdalny zapis lustrzany źródła ładowania systemu może zostać wyłączony z DST lub SST. Wyłączenie zdalnego zapisu lustrzanego źródła ładowania systemu nie jest jednak możliwe, jeśli w systemie znajduje się jednostka dyskowa źródła ładowania systemu, która nie jest podłączona do procesora MFIOP. Jeśli obsługa zdalnego zapisu lustrzanego źródła ładowania systemu jest już wyłączona, przy próbie jej wyłączenia wyświetli się komunikat informujący o tym, że obsługa ta została już wyłączona.

Aby wyłączyć obsługę zdalnego zapisu lustrzanego źródła ładowania systemu, wykonaj następujące czynności:

1. Z głównego menu DST wybierz opcję 4, Praca z jednostkami dyskowymi.
2. Z menu Praca z jednostkami dyskowymi (Work with disk units) wybierz opcję 1, Praca z konfiguracją dysków.
3. Z menu Praca z konfiguracją dysków (Work with disk configuration) wybierz opcję 4, Praca z zabezpieczeniem przez zapis lustrzany.
4. Z menu Praca z zabezpieczeniem przez zapis lustrzany (Work with Mirrored Protection) wybierz opcję 5, Wyłączenie zdalnego zapisu lustrzanego źródła ładowania systemu. Spowoduje to wyświetlenie ekranu potwierdzenia Wyłączenie zdalnego zapisu lustrzanego źródła ładowania systemu (Disable remote load source mirroring).
5. Na ekranie tym naciśnij klawisz Enter. U dołu ekranu Praca z zabezpieczeniem przez zapis lustrzany (Work with mirrored protection) wyświetli się komunikat o wyłączeniu zdalnego zapisu lustrzanego źródła ładowania systemu.

***Użycie zdalnego zapisu lustrzanego źródła ładowania systemu z lokalnymi DASD:*** Zdalny zapis lustrzany źródła ładowania systemu może zostać użyty do osiągnięcia zabezpieczenia pary lustrzanej źródła ładowania systemu na poziomie IOP lub magistrali, nawet bez zdalnego DASD lub magistral. Nie trzeba wykonywać żadnych szczególnych czynności konfiguracyjnych, wystarczy sprawdzić, czy do innego IOP lub magistrali w systemie dołączono jednostkę dyskową o tej samej pojemności co źródło ładowania systemu. Aby uzyskać zabezpieczenie na poziomie magistrali wszystkich par lustrzanych w puli dyskowej, należy skonfigurować system tak, aby nie więcej niż połowa DASD każdej pojemności w danej puli dyskowej była podłączona do jednej magistrali. Aby uzyskać zabezpieczenie na poziomie procesora IOP wszystkich lustrzanych par w puli dyskowej, należy skonfigurować system tak, aby nie więcej niż połowa DASD każdej pojemności w danej puli dyskowej była podłączona do jednego IOP.

Po poprawnym skonfigurowaniu sprzętu systemu można włączyć zabezpieczenie przez zdalny zapis lustrzany źródła ładowania systemu dla pul(i) dyskowych, które mają być chronione. W tym celu należy użyć normalnej funkcji uruchamiania zapisu lustrzanego i normalnej funkcji uruchamiania zabezpieczenia przez zapis lustrzany. Nie ma specjalnych funkcji uruchamiania zabezpieczenia dla obsługi zdalnego źródła ładowania systemu. System wykryje, że zdalny zapis lustrzany źródła ładowania systemu jest aktywny i automatycznie utworzy odpowiednie pary jednostek dyskowych w celu osiągnięcia najlepszego poziomu zabezpieczenia. Ograniczenia normalnego zabezpieczenia przez zapis lustrzany dotyczące łącznej pojemności puli dyskowej, parzystej liczby jednostek dyskowych o każdej pojemności i inne ograniczenia, dotyczą również zabezpieczenia przez zdalny zapis lustrzany.

## Zdalny zapis lustrzany DASD – zalety

- Źródło ładowania systemu może zostać zabezpieczone na poziomie IOP lub magistrali, dzięki użyciu zdalnego zapisu lustrzanego DASD.
- DASD można podzielić między dwa miejsca, tworząc zapis lustrzany jednego na drugim, i w ten sposób uzyskać zabezpieczenie przed awarią, która może wystąpić w jednej z nich.

## Zdalny zapis lustrzany DASD – wady

- System, w którym działa zdalny zapis lustrzany DASD, jest zdolny do wykonania IPL tylko z jednego DASD z pary lustrzanej źródła ładowania systemu. Jeśli DASD ulegnie awarii i nie będzie można powtórzyć par, system nie zdoła wykonać IPL aż do momentu naprawy uszkodzonego źródła ładowania i zdalnego wykonania procedury odzyskania źródła ładowania.
- Jeśli w systemie działa zdalny zapis lustrzany DASD i źródło ładowania systemu, z którego można wykonać IPL zostanie uszkodzone, nie można wykonać zrzutu pamięci głównej w przypadku nienormalnego zakończenia działania systemu. Oznacza to, że system nie może użyć zrzutu pamięci głównej lub funkcji pamięci głównej zasilanej w sposób ciągły (CPM) do zredukowania czasu odzyskiwania po załamaniu systemu. Oznacza to również, że nie można użyć zrzutu pamięci głównej do określenia przyczyny nienormalnego zakończenia działania systemu.

## Porównanie zarządzania DASD w przypadku zwykłego i zdalnego zapisu lustrzanego

W większej części sposób zarządzania zdalnymi kopiami lustrzanymi DASD nie różni się od zarządzania dyskami z lokalnymi kopiami. Jedyne różnice dotyczą dodawania jednostek dyskowych oraz przywracania zabezpieczenia przez zapis lustrzany po odzyskaniu.

***Dodawanie jednostek dyskowych:*** Niezabezpieczone jednostki dyskowe muszą być dodawane parami, jak w przypadku zwykłego zapisu lustrzanego. Aby uzyskać zdalne zabezpieczenie wszystkich dodawanych jednostek, połowa z nich, z każdej pojemności DASD, powinna być w grupie zdalnej, a połowa – w grupie lokalnej. Pojedyncze jednostki chronione przez kontrolę parzystości można dodawać do pul dyskowych z włączonym zdalnym zapisem lustrzanym. Jednakże pula dyskowa nie będzie zabezpieczona na wypadek katastrofy.

***Przywracanie zabezpieczenia przez zapis lustrzany po odzyskaniu:*** Aby przywrócić zabezpieczenie przez zapis lustrzany po procedurze odzyskania, należy wykonać następujące czynności:

- uzyskać i fizycznie podłączyć wszystkie wymagane jednostki DASD,
- zatrzymać lub zawiesić zabezpieczenie przez zapis lustrzany, jeśli jest ono aktualnie skonfigurowane w systemie,
- dodać nowe jednostki DASD do odpowiednich pul dyskowych,
- ponownie uruchomić zabezpieczenie przez zapis lustrzany.

Więcej szczegółowych informacji na temat odzyskiwania danych w systemach z zabezpieczeniem przez zapis lustrzany zawiera książka Składowanie i odtwarzanie  .

## Przygotowanie systemu do zdalnego zabezpieczenia przez zapis lustrzany

Po uruchomieniu zdalnego zapisu lustrzanego tworzone są kopie lustrzane dysków lokalnych na dyskach zdalnych. W przypadku utraty systemu lokalnego bądź zdalnego kopia wszystkich danych systemu

pozostanie dostępna, konfiguracja systemu będzie mogła zostać odzyskana, a przetwarzanie będzie kontynuowane. Aby uchronić się przed awarią całego ośrodka, wszystkie DASD we wszystkich pulach dyskowych systemu muszą mieć zdalną kopię lustrzaną. Aby przygotować system do zdalnego zapisu lustrzanego, wykonaj następujące czynności:

1. Zaplanuj, na których magistralach optycznych będą znajdować się DASD w miejscu zdalnym.
   - Lokalnie i zdalnie nie musi być tyle samo magistral, jednak konfigurowanie systemu jest łatwiejsze, gdy liczba magistral zdalnych i lokalnych oraz liczba DASD są równe.
   - Wymaga się, aby miejsce lokalne i zdalne miały te same pojemności DASD w każdej puli dyskowej.
2. Zaplanuj dystrybucję DASD, przenieś DASD, jeśli jest to konieczne, i sprawdź, czy połowa każdej z pojemności DASD w każdej puli dyskowej została podłączona do lokalnego i zdalnego zestawu magistral.
3. Poinformuj system, które magistrale obsługują dyski lokalne, a które dyski zdalne. W tym celu sprawdź, które magistrale obsługują dyski zdalne i zapisz numery tych magistral. Następnie zmień systemowe nazwy zasobów magistral zdalnych, tak aby zaczynały się od *R*.

   Jeśli na przykład zdalny dysk jest dołączony do magistrali BUS11, zmień systemowy identyfikator zasobu tej magistrali na *RBUS11*.

***Znajdowanie zdalnych magistrali:*** Jeśli magistrale nie zostały oznaczone etykietami, może zaistnieć potrzeba prześledzenia, które magistrale prowadzą do miejsca zdalnego. Za pomocą funkcji Menedżer serwisu sprzętu (Hardware Service Manager) można określić, do której z jednostek rozszerzeń biegnie każda z magistral.

Aby użyć Menedżera serwisu sprzętu w celu sprawdzenia, które magistrale obsługują zdalny DASD, wykonaj następujące kroki:

1. Z głównego menu DST wybierz opcję 7 (Uruchomienie narzędzi serwisowych).
2. Z ekranu Uruchomienie narzędzia serwisowego (Start a Service Tool) wybierz opcję 4 (Menedżer serwisu sprzętu).
3. Z menu Menedżer serwisu sprzętu (Hardware Service Manager) wybierz opcję 2 (Logiczne zasoby sprzętowe).
4. Z menu Logiczne zasoby sprzętowe (Logical hardware resources) wybierz opcję 1 (Zasoby magistrali systemowych).
5. Na ekranie Logiczne zasoby sprzętowe na magistrali systemu (Logical hardware resource on system bus) przed każdą magistralą wpisz opcję 8, aby wyświetlić związane z nią zasoby pakietu.
6. Ekran zasobów pakietu, które są powiązane z danym zasobem logicznym, przedstawia ID ramki i nazwę zasobu jednostki rozszerzeń przyłączonej do danej magistrali. Jeśli chcesz uzyskać więcej informacji, wpisz opcję 5 obok pozycji Jednostka rozszerzeń systemu, aby wyświetlić dalsze szczegóły na temat jednostki rozszerzeń.

   Zapisz zdalną lub lokalną jednostkę logiczną magistrali. Powtórz tę procedurę dla wszystkich magistral systemu.

***Zmiana nazw zasobów zdalnych magistral:*** Kiedy wiadomo już, na których magistralach znajdują się zdalne DASD, należy użyć funkcji Menedżer serwisu sprzętu (Hardware Service Manager), aby zmienić nazwy zasobów zdalnych magistral.

Aby zmienić nazwy zasobów zdalnych magistrali, wykonaj następujące kroki:

1. Z głównego menu DST wybierz opcję 7 (Uruchomienie narzędzi serwisowych).
2. Z ekranu Uruchomienie narzędzia serwisowego (Start a Service Tool) wybierz opcję 4 (Menedżer serwisu sprzętu).
3. Z menu Menedżer serwisu sprzętu (Hardware Service Manager) wybierz opcję 2 (Logiczne zasoby sprzętowe).
4. Z menu Logiczne zasoby sprzętowe (Logical hardware resources) wybierz opcję 1 (Zasoby magistrali systemowych).

5. Na ekranie Logiczne zasoby sprzętowe na magistrali systemu (Logical hardware resource on system bus) zaznacz za pomocą opcji 2 magistralę, której nazwę chcesz zmienić. Wyświetlony zostanie ekran Zmiana szczegółów logicznych zasobów sprzętu (Change logical hardware resource detail).
6. Na ekranie Zmiana szczegółów logicznego zasobu sprzętowego (Change logical hardware resource detail), w wierszu o nazwie Nowa nazwa zasobu, zmień nazwę zasobu, dodając literę *R* na początku nazwy zasobu magistrali; na przykład zmień *BUS08* na *RBUS08*. Naciśnij Enter, aby zmienić nazwę zasobu.

   Powtórz tę procedurę dla każdej zdalnej magistrali w systemie.

## Rozpoczynanie zdalnego zapisu lustrzanego

Po zakończeniu przygotowania systemu, w celu rozpoczęcia zdalnego zapisu lustrzanego wykonaj następujące czynności:

1. Włącz zdalny zapis lustrzany jednostki ładowania systemu. Umożliwi to włączenie jednostki ładowania systemu do zdalnej grupy dysków.
2. Użyj normalnej funkcji uruchamiania zapisu lustrzanego.

   Po uruchomieniu zapisu lustrzanego system użyje nazw zasobów do określenia, które magistrale są zdalne, a następnie spróbuje połączyć w pary DASD znajdujące się na magistralach zdalnych i lokalnych. Ponieważ zapis lustrzany zdalnej jednostki ładowania systemu jest włączony, system połączy w pary ze zdalnym DASD również jednostkę ładowania systemu. Ograniczenia normalnego zabezpieczenia przez zapis lustrzany dotyczące łącznej pojemności puli dyskowej, parzystej liczby jednostek dyskowych o każdej pojemności i inne ograniczenia, dotyczą również zabezpieczenia przez zdalny zapis lustrzany.
3. Na ekranie potwierdzenia uruchomienia zapisu lustrzanego sprawdź, czy wszystkie pary lustrzane mają poziom zabezpieczenia *Magistrala zdalna*. Określ, dlaczego niektóre jednostki mają niższy poziom zabezpieczenia, rozwiąż problem, a następnie ponownie spróbuj uruchomić zabezpieczenie przez zapis lustrzany.

# Rozdział 2. Wybór poziomu zabezpieczenia

Istnieje kilka sposobów takiego skonfigurowania systemu, aby wykorzystać funkcje zabezpieczenia dysków. Przed wybraniem potrzebnych opcji zabezpieczenia dysków należy porównać stopień zabezpieczenia, jaki zapewniają.

- Porównanie opcji zabezpieczenia dysków
- Pełne zabezpieczenie przez zapis lustrzany a częściowe zabezpieczenie przez zapis lustrzany

Po porównaniu opcji zabezpieczenia dysków należy wybrać jedną z poniższych metod ich użycia:

- Pełne zabezpieczenie — pojedyncza pula dyskowa
- Pełne zabezpieczenie — wiele pul dyskowych
- Częściowe zabezpieczenie — wiele pul dyskowych
- “Przypisanie nowych jednostek dyskowych do pul dyskowych” na stronie 51

## Porównanie opcji zabezpieczenia dysków

Przed wybraniem opcji zabezpieczenia dysków należy zapoznać się z poniższymi uwagami:

- W przypadku awarii pojedynczego dysku zarówno sprzętowe zabezpieczenie przez kontrolę parzystości, jak i zabezpieczenie przez zapis lustrzany sprawiają, że system nadal pracuje. Jeśli używane jest zabezpieczenie przez zapis lustrzany, system może kontynuować pracę po uszkodzeniu elementu związanego z dyskiem, takiego jak kontroler albo procesor IOP.
- Jeśli wystąpi awaria drugiego dysku i w systemie znajdują się dwa uszkodzone dyski, jest bardziej prawdopodobne, że system będzie kontynuował działanie z zabezpieczeniem przez zapis lustrzany niż ze sprzętowym zabezpieczeniem przez kontrolę parzystości. Jeśli stosowane jest sprzętowe zabezpieczenie przez kontrolę parzystości, prawdopodobieństwo zatrzymania systemu w wyniku awarii drugiego dysku można wyrazić jako P do n, gdzie n jest całkowitą liczbą dysków w systemie, a P jest liczbą dysków w zestawie z kontrolą parzystości, w którym była pierwsza awaria. Dla zabezpieczenia przez zapis lustrzany prawdopodobieństwo załamania systemu po wystąpieniu awarii drugiego dysku wynosi 1 do n.
- Sprzętowe zabezpieczenie przez kontrolę parzystości wymaga jednego dysku o takiej samej pojemności, jak inne dyski w zestawie parzystości. Są na nim przechowywane informacje o parzystości. System z zabezpieczeniem przez zapis lustrzany wymaga użycia dysków o dwukrotnie większej pojemności niż ten sam system bez tego zabezpieczenia, ponieważ wszystkie informacje są przechowywane dwukrotnie. Zabezpieczenie przez zapis lustrzany może także wymagać większej liczby magistral, procesorów IOP i kontrolerów dyskowych, w zależności od założonego poziomu ochrony. Dlatego zabezpieczenie przez zapis lustrzany jest przeważnie kosztowniejszym rozwiązaniem niż sprzętowe zabezpieczenie przez kontrolę parzystości.
- Zazwyczaj sprzętowe zabezpieczenie przez kontrolę parzystości i zabezpieczenie przez zapis lustrzany nie mają zauważalnego wpływu na wydajność systemu. W niektórych wypadkach zabezpieczenie przez zapis lustrzany może nawet podnieść wydajność systemu.
- Czas wymagany do odtworzenia danych w jednostkach dyskowych chronionych przez sprzętowe zabezpieczenie przez kontrolę parzystości jest dłuższy niż czas odtwarzania w tych samych napędach dyskowych bez uaktywnionego sprzętowego zabezpieczenia przez kontrolę parzystości, ponieważ dane parzystości muszą być obliczone i zapisane.

Poniższa tabela stanowi przegląd dostępnych na serwerze narzędzi, które mogą być wykorzystane w celu zabezpieczenia go przed różnymi typami awarii.

| Oczekiwany typ dostępności | Sprzętowe zabezpieczenie przez kontrolę parzystości | Zabezpieczenie przez zapis lustrzany | Podstawowe pule dyskowe | Niezależna pula dyskowa |
|---|---|---|---|---|
| Ochrona przed utratą danych w wyniku uszkodzenia sprzętu związanego z dyskiem | Tak | Tak | Patrz uwaga [2] | Patrz uwaga [2] |
| Utrzymanie dostępności | Tak | Tak | Nie | Tak[4] |
| Pomoc przy odzyskiwaniu jednostek dyskowych | Tak | Tak | Tak[2] | Tak[2] |
| Obsługa dostępności w przypadku awarii adaptera wejścia/wyjścia (IOA) | Nie | Tak[1] | Nie | Nie |
| Utrzymanie dostępności w razie awarii procesora we/wy | Nie | Tak[1] | Nie | Nie |
| Obsługa dostępności w przypadku awarii magistrali systemowej | Nie | Tak[1] | Nie | Nie |
| Ochrona przed całkowitym zniszczeniem | Nie | Tak[3] | Nie | Nie |
| Zdolność do przełączania danych pomiędzy systemami | Nie | Nie | Nie | Tak |

**Uwaga:**

[1] Zależy od używanego sprzętu, konfiguracji oraz poziomu zabezpieczenia przez zapis lustrzany.

[2] Skonfigurowanie pul dyskowych może ograniczyć utratę danych oraz ich odzyskiwanie do pojedynczej puli dyskowej.

[3] Do zabezpieczenia miejsca przed całkowitą utratą danych wymagany jest zdalny zapis lustrzany.

[4] W środowisku z klastrami niezależna pula dyskowa może pomóc w obsłudze dostępności.

Patrz także:

- “Jak system zarządza pamięcią dyskową” na stronie 47
- “Jak konfiguruje się dyski” na stronie 47

## Pełne zabezpieczenie przez zapis lustrzany a częściowe zabezpieczenie przez zapis lustrzany

Zastosowanie albo pełnego zabezpieczenia przez zapis lustrzany albo częściowego zabezpieczenie przez zapis lustrzany skutkuje uzyskaniem odmiennej dostępności. Te dwie implementacje zabezpieczenia przez zapis lustrzany są zupełnie różne. Scenariusze jednostki dyskowej w serwerze iSeries dla każdej z tych metod zapisu lustrzanego wymagają innych odpowiedzi użytkownika.

Bez względu na to, czy używana jest tylko systemowa pula dyskowa (pula dyskowa 1) czy kilka pul dyskowych użytkowników (od 2 do 255), pełne zabezpieczenie przez zapis lustrzany chroni wszystkie jednostki dyskowe w serwerze iSeries. Częściowe zabezpieczenie przez zapis lustrzany chroni tylko część jednostek dyskowych w jednej lub kilku pulach dyskowych. Jednakże nie wszystkie jednostki w konfiguracji dysku są chronione. Dlatego planowanie rozmieszczenia jednostek dyskowych i wybór pul dyskowych dla zabezpieczenia przez zapis lustrzany staje się bardziej skomplikowane.

Poza planowaniem pul dyskowych znaczna różnica pomiędzy dwoma metodami zabezpieczenia przez zapis lustrzany dotyczy poziomu dostępności. W przypadku zabezpieczenia przez zapis lustrzany użytkownik maksymalizuje dostępność serwera iSeries w momencie wystąpienia awarii podsystemu dysków. Przy użyciu tej metody zabezpieczenia przez zapis lustrzany nie ma znaczenia, która pula dyskowa uległa awarii. W częściowym zabezpieczeniu przez zapis lustrzany system nadal działa, zgłaszając uszkodzoną jednostkę pamięci do kolejki komunikatów operatora systemu (QSYSOPR). Jednakże jeśli awaria dysku wystąpi w puli dyskowej bez zabezpieczenia przez zapis lustrzany, gdy zadanie w systemie odwoła się do tej puli

dyskowej, wysyłany jest kod SRC A6xx 0266. Ponieważ jednostki pamięci nie mają jednostek lustrzanych, katalog zarządzania pamięcią staje się bezużyteczny i wszystkie operacje wejścia i wyjścia do puli dyskowej są wstrzymywane.

Kod SRC nie oznacza końca pracy systemu. Wszystkie operacje wejścia i wyjścia są zapisywane w kolejce, co umożliwia Inżynierowi Serwisu określenie przyczyny awarii dysku. Jeśli problem nie dotyczy dysku, wadliwe karty są wymieniane, uszkodzona jednostka dyskowa jest uruchamiana i system kontynuuje działanie od punktu wystąpienia błędu sprzętu. Wznawiane są wszystkie zapisane w kolejce operacje wejścia i wyjścia. Jednakże jeśli wystąpi awaria dysku, Inżynier Serwisu wykonuje zrzut pamięci głównej, aby zminimalizować czas następnego IPL do OS/400 i umożliwia systemowi zakończenie przetwarzania.

W przypadku pełnego zabezpieczenia przez zapis lustrzany działanie systemu nie jest przerywane podczas diagnostyki ani podczas przeprowadzania większości napraw mających na celu usunięcie awarii podsystemu dysków. W przypadku zabezpieczenia na poziomie procesora we/wy, w zależności od błędu, możliwa jest maksymalna jednoczesna konserwacja. W każdym przypadku użytkownik może wyłączyć system, aby usunąć problem związany z dyskiem; system zakończy pracę normalnie.

Chociaż dane krytyczne są zabezpieczone za pomocą częściowego zabezpieczenia przez zapis lustrzany i nie wymaga się odtwarzania danych w zabezpieczonej puli dyskowej, trudno osiągnąć maksymalną dostępność, jaką zapewnia pełne zabezpieczenie przez zapis lustrzany, a to z powodu dostępnej niezabezpieczonej puli dyskowej. Jeśli wymagania dotyczące dostępności mówią, że system musi nim wystąpi awaria działać przez kilka minut, lub pozostawać aktywny podczas godzin pracy, w większości przypadków częściowe zabezpieczenie przez zapis lustrzany staje się bezużyteczne.

## Jak system zarządza pamięcią dyskową

Aby zrozumieć opcję dostępności w serwerze, należy wykazać się podstawowym zrozumieniem sposobu, w jaki serwer iSeries zarządza pamięcią dyskową. Pamięć w serwerze jest nazywana **pamięcią główną**. Pamięć dyskowa (pomocnicza) jest nazywana po prostu **pamięcią**. Pamięć dyskowa bywa także określana jako **DASD (direct access storage device)**, czyli urządzenie pamięci o dostępie bezpośrednim.

W wielu innych systemach komputerowych użytkownik odpowiada za to, w jaki sposób dane są przechowywane na dyskach. Tworząc nowy plik, musi ustalić, gdzie ma on zostać umieszczony w systemie i jaką ma mieć wielkość. Aby zapewnić dobrą wydajność systemu, musi umieścić pliki na odpowiednich dyskach. Jeśli później okaże się, że plik powinien być większy, musi przenieść go w takie miejsce na dysku, które ma dostatecznie dużo przestrzeni dla nowego, większego pliku. Być może trzeba będzie przenosić pliki pomiędzy jednostkami dyskowymi, aby utrzymać wydajność systemu.

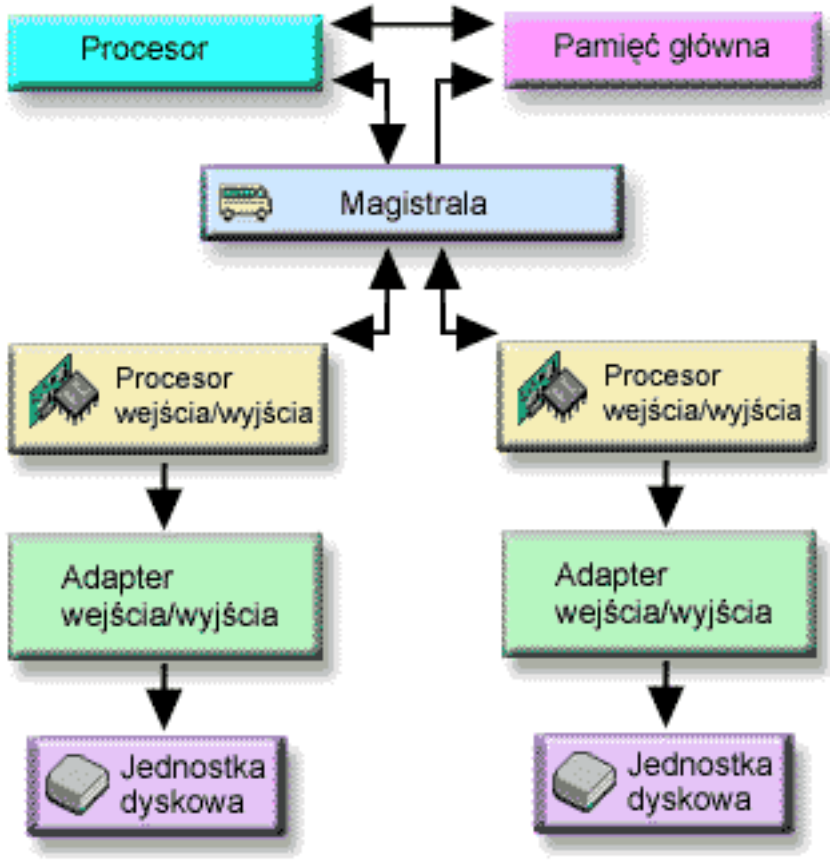
Serwer iSeries wyróżnia się sposobem przejmowania odpowiedzialności za zarządzanie informacjami w pamięci dyskowej. Tworząc plik, podaje się szacunkową liczbę rekordów, jaką powinien on zawierać. System umieszcza ten plik w miejscu najlepszym z punktu widzenia wydajności. W rzeczywistości dane mogą zostać rozproszone po kilku jednostkach dyskowych. Podczas dodawania kolejnych rekordów do pliku system przydziela dodatkową przestrzeń na jednej lub kilku jednostkach dyskowych.

**Pamięć pojedynczego poziomu** jest unikalną architekturą serwera iSeries umożliwiającą dokładną i wydajną współpracę pamięci głównej i pamięci dyskowej. Dysponując pamięcią pojedynczego poziomu programy i użytkownicy systemu proszą o dane na podstawie nazwy, a nie na podstawie fizycznego położenia danych. System przechowuje ścieżkę do najnowszej kopii każdego elementu informacji w pamięci głównej lub pamięci dyskowej.

## Jak konfiguruje się dyski

System wykorzystuje wiele elementów elektronicznych do zarządzania przesyłaniem danych z dysku do pamięci głównej. Dane i programy muszą znajdować się w pamięci głównej, zanim zostaną użyte. Poniższa

ilustracja przedstawia sprzęt używany do przesyłania danych:




***Magistrala:*** Magistrala jest głównym kanałem transmisji danych wejściowych i wyjściowych. System może mieć więcej niż jedną magistralę.

***Procesor we/wy:*** Procesor wejścia/wyjścia (IOP) przyłączony do magistrali. IOP jest używany do przekazywania informacji pomiędzy pamięcią główną i określonymi grupami kontrolerów. Niektóre IOP są przeznaczone dla określonych typów kontrolerów, takich jak kontrolery dysków. Do innych IOP można przyłączyć kilka rodzajów kontrolerów, na przykład kontrolery napędów taśm i dysków.

***Adapter wejścia/wyjścia (IOA):*** Adapter IOA jest podłączany do procesora IOP i obsługuje przesyłanie informacji pomiędzy IOP a jednostkami dyskowymi.

***Jednostka dyskowa:*** Jednostki dyskowe to właściwe urządzenia, które zawierają jednostki pamięci. Sprzęt zamawia się na poziomie jednostek dyskowych. Każda jednostka dyskowa ma własny numer seryjny. Poniższe informacje opisują, jak serwer adresuje poszczególne jednostki pamięci.

## Sposób adresowania przez system poszczególnych jednostek dyskowych

Aby przenosić dane do pamięci pomocniczej i odwrotnie, system musi mieć możliwość identyfikowania pojedynczych jednostek pamięci. Każdy element sprzętu (magistrala, procesor wejścia/wyjścia, kontroler oraz jednostki pamięci) ma swój unikalny adres.

Adres jednostki pamięci składa się z magistrali systemowej, płyty systemowej, karty systemowej, magistrali we/wy, kontrolera oraz numerów urządzenia.

```
   Szczegółowe informacje dotyczące zasobów sprzętowych jednostek dyskowych
            (Disk Unit Hardware Resource Information Details)

Typ..............: 6603
Model............: 030
Numer seryjny....: 00-0109928
Nazwa zasobu.....: DD002

Magistrala SPD
 Magistrala systemowa.:   1
 Płyta systemowa......:   0
 Karta systemowa......:   1

Pamięć
 Magistrala we/wy.....:   0
 Kontroler............:   1
 Urządzenie...........:   0
```

## Pełne zabezpieczenie – pojedyncza pula dyskowa

Najprostszym sposobem zarządzania i zabezpieczenia pamięci dyskowej jest:

- przypisanie wszystkich jednostek dyskowych do pojedynczej puli dyskowej (systemowa pula dyskowa),
- zastosowanie sprzętowego zabezpieczenia przez kontrolę parzystości dla wszystkich jednostek dyskowych, które mają odpowiednie możliwości sprzętowe,
- użycie zabezpieczenia przez zapis lustrzany dla pozostałych jednostek dyskowych systemu.

Po zastosowaniu tej metody, jeśli wystąpi awaria pojedynczej jednostki dyskowej, system będzie nadal działał. Po wymianie uszkodzonego dysku system odtwarza informacje, aby żadne dane nie zostały utracone. System może również kontynuować działanie w razie uszkodzenia elementu związanego z dyskiem. To, czy system będzie kontynuował działanie, zależy od zastosowanej konfiguracji. Na przykład system będzie kontynuował działanie, jeśli uszkodzeniu ulegnie procesor IOP, a pary lustrzane wszystkich przyłączonych do niego jednostek dyskowych zostaną przyłączone do innego procesora IOP.

Jeśli w celu pełnego zabezpieczenia systemu używane jest połączenie zabezpieczenia przez zapis lustrzany i sprzętowego zabezpieczenia przez kontrolę parzystości, zapotrzebowanie na przestrzeń dyskową jest większe. Sprzętowe zabezpieczenie przez kontrolę parzystości wymaga do 25% dodatkowej przestrzeni na jednostkach dyskowych do przechowywania informacji dotyczących parzystości. Zabezpieczenie przez zapis lustrzany wymaga podwojenia pojemności wszystkich dysków, dla których nie jest aktywne sprzętowe zabezpieczenie przez kontrolę parzystości.

## Pełne zabezpieczenie – wiele pul dyskowych

Użytkownik może chcieć podzielić jednostki dyskowe na kilka pul dyskowych (pul pamięci dyskowej). Czasami wydajność całego systemu wzrasta dzięki pulom dyskowym użytkowników. Na przykład po wydzieleniu dzienników w podstawowej lub dodatkowej puli dyskowej. Pliki historii lub dokumenty, które rzadko się zmieniają, można umieścić w puli dyskowej zawierającej jednostki dyskowe o mniejszej wydajności.

Aby w pełni zabezpieczyć system zawierający wiele pul dyskowych, należy podjąć takie działania jak:

- Zastosowanie sprzętowego zabezpieczenia przez kontrolę parzystości dla wszystkich jednostek dyskowych, które mają odpowiednie możliwości sprzętowe.
- Skonfigurowanie zabezpieczenia przez zapis lustrzany dla wszystkich pul dyskowych w systemie. Można skonfigurować zabezpieczenie przez zapis lustrzany nawet dla puli dyskowej zawierającej wyłącznie jednostki dyskowe ze sprzętowym zabezpieczeniem przez kontrolę parzystości. W ten sposób jednostki dodawane w przyszłości, które nie będą miały sprzętowego zabezpieczenia przez kontrolę parzystości, będą automatycznie zabezpieczane przez zapis lustrzany.

**Uwaga:** W przypadku zabezpieczenia przez zapis lustrzany należy dodać nowe jednostki w parach o równej pojemności.

Przed konfigurowaniem tego poziomu zabezpieczenia należy dowiedzieć się, jak przypisać jednostki dyskowe do pul dyskowych.

## Częściowe zabezpieczenie – wiele pul dyskowych

Czasami pełne zabezpieczenie (wykorzystujące kombinację: sprzętowe zabezpieczenie przez kontrolę parzystości oraz zabezpieczenie przez zapis lustrzany) może być zbyt kosztowne. W takim wypadku należy wypracować strategię ochrony informacji o największym znaczeniu. Podstawowymi założeniami powinny być: zminimalizowanie utraty danych oraz skrócenie czasu, w którym aplikacje o podstawowym znaczeniu nie są dostępne. Właściwą strategią będzie prawdopodobnie podzielenie systemu na podstawowe lub niezależne pule dyskowe i zabezpieczenie tylko wybranych pul dyskowych. Należy jednak wziąć pod uwagę fakt, że system nie jest w pełni zabezpieczony i jeśli ulegnie awarii niezabezpieczona jednostka dyskowa, mogą się pojawić poważne problemy. Cały system może: przestać działać, zakończyć nienormalnie pracę, wymagać długiego odzyskiwania, a dane znajdujące się w puli dyskowej, zawierającej uszkodzoną jednostkę, będą musiały zostać odtworzone.

Przed konfigurowaniem tego poziomu zabezpieczenia należy dowiedzieć się, jak przypisać jednostki dyskowe do pul dyskowych.

Poniżej została przedstawiona lista zaleceń dotyczących tworzenia strategii:

- Jeśli systemowa pula dyskowa jest zabezpieczona kombinacją: zabezpieczenie przez zapis lustrzany i sprzętowe zabezpieczenie przez kontrolę parzystości, można skrócić lub całkowicie wyeliminować czas odzyskiwania. Systemowa pula dyskowa, a w szczególności jednostka ładowania systemu, zawierają informacje o kluczowym znaczeniu dla utrzymania działania systemu. Na przykład systemowa pula dyskowa zawiera informacje o ochronie, informacje o konfiguracji oraz adresy wszystkich bibliotek systemowych.
- Należy wziąć pod uwagę sposób odzyskiwania informacji o obiekcie. Jeśli istnieją działające aplikacje i obiekty stale ulegają zmianom, należy rozważyć użycie kronikowania i umieszczenia dzienników w zabezpieczonej puli pamięci użytkowników.
- Należy przeanalizować, które informacje nie wymagają ochrony, prawdopodobnie wskutek rzadko wprowadzanych zmian. Na przykład zbiory historii mogą wymagać ciągłego dostępu, ale znajdujące się w nich dane mogą zmieniać się co najwyżej pod koniec miesiąca. Można umieścić te zbiory w oddzielnej puli dyskowej, nieposiadającej żadnego zabezpieczenia dysków. W przypadku awarii system będzie niezdatny do użytku, ale dane można będzie odtworzyć w całości. W taki sam sposób można postąpić z dokumentami.
- Należy wziąć pod uwagę inne informacje, które nie wymagają zabezpieczenia dysku. Na przykład programy użytkowe mogą znajdować się w innej bibliotece niż przeznaczone dla nich dane. Prawdopodobnie programy są rzadko modyfikowane. Biblioteki programów mogą być umieszczone w niezabezpieczonej podstawowej puli dyskowej. W przypadku awarii system będzie niezdatny do użytku, ale programy można będzie odtworzyć.

Powyższe wskazówki można ująć w dwóch prostych zaleceniach:

1. Aby zmniejszyć czas odzyskiwania, należy zabezpieczyć systemową pulę dyskową.
2. Aby zminimalizować utratę danych, należy zdecydować, które biblioteki i obiekty muszą być zabezpieczone.

## Przypisanie nowych jednostek dyskowych do pul dyskowych

Jeśli użytkownik chce mieć kilka pul dyskowych, zwanych również pulami pamięci dyskowej (ASP) w interfejsie znakowym, dla każdej puli należy określić:

- wielkość wymaganej pamięci,
- rodzaj stosowanego zabezpieczenia dysków, jeśli ma być ono używane,
- jednostki dyskowe, które mają być przypisane,
- obiekty, które mają być umieszczone w puli dyskowej.

Książka Workstation Customization Programming  zawiera informacje, które pomogą podjąć te decyzje.

Podczas pracy z konfiguracją dysków może pomóc wydrukowanie konfiguracji własnego systemu. Informacje na ten temat można uzyskać z Hardware Service Manager w narzędziach SST lub z folderu Disk Units w iSeries Navigator.