**Typy kopii bezpieczeństwa, strategie tworzenia kopii bezpieczeństwa**

Ochrona danych przed utratą, zniszczeniem, katastrofami (spowodowanymi przez człowieka lub przyczyny naturalne) i innymi problemami jest jednym z głównych priorytetów organizacji IT. W koncepcji pomysły są proste, chociaż wdrażanie wydajnego i efektywny zestaw operacji tworzenia kopii zapasowych może być trudny.

Termin „kopia zapasowa" stał się synonimem ochrony danych w ciągu ostatnich kilkudziesięciu lat i można go wykonać kilkoma metodami. Aplikacje oprogramowania do tworzenia kopii zapasowych zmniejszają złożoność wykonywania operacji tworzenia kopii zapasowych i odzyskiwania.

Tworzenie kopii zapasowych danych jest tylko częścią planu ochrony przed katastrofami i może nie zapewnić wymaganego poziomu danych i funkcji odtwarzania po awarii bez starannego projektowania i testowania.

Aplikacje do tworzenia kopii zapasowych od dawna oferują kilka typów operacji tworzenia kopii zapasowych. Do najczęstszych typów kopii zapasowych stanowią pełnej kopii zapasowej, przyrostowych kopii zapasowych i różnicowa kopia zapasowa. Inne typy kopii zapasowych obejmują syntetyczne pełne kopie zapasowe i dublowanie.

W debacie na temat kopii zapasowych w chmurze i lokalnych, istnieją pewne typy kopii zapasowych, które są lepsze w niektórych lokalizacjach. Jeśli tworzysz kopię zapasową w chmurze, przyrostowe kopie zapasowe są ogólnie lepszym rozwiązaniem, ponieważ zużywają mniej zasobów. Możesz zacząć od pełnej kopii zapasowej w chmurze, a następnie przejść do tworzenia przyrostowych kopii zapasowych.

Kopia lustrzana jest jednak zazwyczaj bardziej podejściem lokalnym i często obejmuje dyski.

**1. Pełne kopie zapasowe**

Najbardziej podstawowym i kompletnym typem operacji tworzenia kopii zapasowych jest pełna kopia zapasowa. Jak sama nazwa wskazuje, ten typ kopii zapasowej tworzy kopię wszystkich danych na urządzeniu magazynującym, takim jak dysk lub taśma. Podstawową zaletą wykonywania pełnej kopii zapasowej podczas każdej operacji jest to, że pełna kopia wszystkich danych jest dostępna na jednym zestawie nośników. Zapewnia to minimalny czas na przywrócenie danych, miernik znany jako docelowy czas odtwarzania. Jednak wady polegają na tym, że wykonanie pełnej kopii zapasowej zajmuje więcej czasu niż w przypadku innych typów (czasami o współczynnik 10 lub więcej) i wymaga więcej miejsca w pamięci.

Dlatego pełne kopie zapasowe są zwykle uruchamiane tylko okresowo. Centra danych, które mają niewielką ilość danych (lub krytyczne aplikacje), mogą codziennie lub nawet częściej wykonywać pełną

kopię zapasową. Zwykle operacje tworzenia kopii zapasowych wykorzystują pełną kopię zapasową w połączeniu z kopiami przyrostowymi lub różnicowymi.

**2. Przyrostowe kopie zapasowe**

Operacja przyrostowej kopii zapasowej spowoduje skopiowanie tylko tych danych, które uległy zmianie od czasu ostatniej operacji tworzenia kopii zapasowej dowolnego typu. Organizacja zwykle używa zmodyfikowanego znacznika czasu na plikach i porównuje go ze znacznikiem czasu ostatniej kopii zapasowej. Aplikacje do tworzenia kopii zapasowych śledzą i rejestrują datę i godzinę wykonania operacji tworzenia kopii zapasowych w celu śledzenia plików zmodyfikowanych od czasu tych operacji. Ponieważ przyrostowa kopia zapasowa kopiuje tylko dane od ostatniej kopii zapasowej dowolnego typu, organizacja może ją uruchamiać tak często, jak jest to potrzebne, z zachowaniem tylko najnowszych zmian. Zaletą przyrostowej kopii zapasowej jest to, że kopiuje ona mniejszą ilość danych niż pełna. W związku z tym operacje te będą miały większą szybkość tworzenia kopii zapasowych i będą wymagały mniej nośników do przechowywania kopii zapasowej.

**3. Kopie różnicowe**

Operacja różnicowej kopii zapasowej jest podobna do operacji przyrostowej podczas jej pierwszego wykonywania, ponieważ kopiuje wszystkie dane zmienione w stosunku do poprzedniej kopii zapasowej. Jednak za każdym razem, gdy jest uruchamiany później, będzie kontynuował kopiowanie wszystkich danych zmienionych od czasu poprzedniej pełnej kopii zapasowej. W związku z tym podczas kolejnych operacji będzie przechowywać więcej kopii zapasowych niż danych przyrostowych, chociaż zazwyczaj jest to znacznie mniej niż pełna kopia zapasowa. Co więcej, różnicowe kopie zapasowe wymagają więcej miejsca i czasu do wykonania niż przyrostowe kopie zapasowe, chociaż mniej niż pełne kopie zapasowe.

**A comparison of different types of backup**

| TYPE/BACKUP | FULL | MIRROR | INCREMENTAL | DIFFERENTIAL |
|---|---|---|---|---|
| Backup 1 | All data | All data selected | – | – |
| Backup 2 | All data | All data selected | Changes from backup 1 | Changes from backup 1 |
| Backup 3 | All data | All data selected | Changes from backup 2 | Changes from backup 1 |
| Backup 4 | All data | All data selected | Changes from backup 3 | Changes from backup 1 |



Tabela 1: Porównanie różnych typów kopii zapasowych

Jak pokazano w powyższej sekcji „Porównanie różnych typów kopii zapasowych”, każdy proces tworzenia kopii zapasowej przebiega inaczej. Organizacja musi przynajmniej raz wykonać pełną kopię zapasową. W przypadku kolejnych kopii zapasowych można uruchomić kolejną pełną, przyrostową lub różnicową kopię zapasową. Pierwsza wykonana częściowa kopia zapasowa, różnicowa lub przyrostowa, utworzy kopię zapasową tych samych danych. W trzeciej operacji tworzenia kopii zapasowej dane, których kopia zapasowa jest tworzona w trybie przyrostowym, są ograniczone do zmian, jakie zaszły od ostatniego tworzenia kopii przyrostowej. Dla porównania trzecia kopia zapasowa z różnicą utworzy kopię zapasową wszystkich zmian od czasu pierwszej pełnej kopii zapasowej, czyli „Kopia zapasowa 1”.
Z tych trzech podstawowych typów kopii zapasowych można opracować podejście do kompleksowej ochrony danych. Organizacja często używa jednego z następujących ustawień kopii zapasowych:

Pełna codziennie
Pełny tydzień + różnica dzienna
Pełny tydzień + przyrostowy dzienny
Wiele czynników wpłynie na wybór optymalnej strategii tworzenia kopii zapasowych. Zazwyczaj każda alternatywa i wybór strategii wiążą się z kompromisami między wydajnością, poziomami ochrony danych, całkowitą ilością zatrzymywanych danych i kosztami. W poniższej sekcji „Wpływ strategii tworzenia kopii zapasowych na przestrzeń” wymagania dotyczące pojemności nośników i nośniki wymagane do odtwarzania są pokazane dla trzech typowych strategii tworzenia kopii zapasowych. Obliczenia te zakładają 20 TB wszystkich danych, przy czym 5% danych zmienia się codziennie i brak wzrostu całkowitej pamięci masowej w tym okresie. Obliczenia opierają się na 22 dniach roboczych w miesiącu i miesięcznym okresie przechowywania danych.

**A backup strategy's impact on space**

| COMMON BACKUP SCENARIOS | MEDIA SPACE REQUIRED FOR ONE MONTH (20 TB @ 5% DAILY RATE OF CHANGE) | MEDIA REQUIRED FOR RECOVERY |
|---|---|---|
| Full daily (weekdays) | Space for 22 daily fulls (22 * 20 TB) = 440.00 TB | Most recent backup only |
| Full (weekly) + Differential (weekdays) | Fulls, plus most recent differential since full (5 * 20 TB) + (22 * 5%* 20 TB) = 122.00 TB | Most recent full + most recent differential |
| Full (weekly) + Incremental (weekdays) | Fulls, plus all incrementals since weekly full (5 * 20 TB) + (22 * 5% * 20 TB) = 122.00 TB | Most recent full + all incrementals since full |



Tabela 2: Wpływ strategii tworzenia kopii zapasowych na przestrzeń
Jak pokazano powyżej, codzienne wykonywanie pełnej kopii zapasowej wymaga największej ilości miejsca, a także zajmuje najwięcej czasu. Jednak dostępnych jest więcej kopii danych, a do wykonania

operacji przywracania potrzeba mniej elementów nośnika. W rezultacie wdrożenie tych zasad tworzenia kopii zapasowych zapewnia większą odporność na awarie i zapewnia najkrótszy czas na przywrócenie, ponieważ wszystkie wymagane dane będą znajdować się w co najwyżej jednym zestawie kopii zapasowych.

Alternatywnie, cotygodniowe wykonywanie pełnej kopii zapasowej w połączeniu z codziennym wykonywaniem przyrostowych kopii zapasowych zapewni najkrótszy czas tworzenia kopii zapasowych w dni powszednie i zużyje najmniej miejsca. Dostępnych jest jednak mniej kopii danych, a czas odtwarzania jest najdłuższy, ponieważ organizacja może potrzebować sześciu zestawów nośników do odzyskania niezbędnych informacji. Jeśli potrzebne są dane z kopii zapasowej danych w środę, wymagana jest pełna kopia zapasowa w niedzielę oraz zestawy nośników przyrostowych z poniedziałku, wtorku i środy. Może to znacznie wydłużyć czas odtwarzania i wymaga prawidłowego działania każdego zestawu nośników; awaria jednego zestawu kopii zapasowych może mieć wpływ na całe przywracanie.

Uruchamianie cotygodniowej pełnej kopii zapasowej oraz dziennych kopii różnicowych zapewnia wyniki pomiędzy innymi alternatywami. Mianowicie, do przywrócenia potrzeba więcej zestawów nośników kopii zapasowych niż w przypadku codziennej pełnej polityki, chociaż mniej niż w przypadku codziennej polityki przyrostowej. Ponadto czas przywracania jest krótszy niż w przypadku codziennych przyrostowych kopii zapasowych i dłuższy niż dziennych pełnych kopii zapasowych. Aby przywrócić dane z określonego dnia, wymagane są co najwyżej dwa zestawy nośników, co skraca czas potrzebny do odzyskania i potencjalne problemy z nieczytelnym zestawem kopii zapasowych.

**4. Kopie lustrzane**

Kopia lustrzana jest porównywalna do pełnej kopii zapasowej. Według bloga dostawcy kopii zapasowych Nakivo : „Ten typ kopii zapasowej tworzy dokładną kopię źródłowego zestawu danych, ale tylko najnowsza wersja danych jest przechowywana w repozytorium kopii zapasowych bez śledzenia różnych wersji plików”. Kopia zapasowa jest lustrem danych źródłowych, a więc wszystkie różne pliki z kopiami zapasowymi są przechowywane osobno, tak jak w źródle.

Jedną z zalet kopii zapasowej lustrzanej jest szybki czas odzyskiwania danych.

Dostęp do poszczególnych plików kopii zapasowych jest również łatwy.

Jedną z głównych wad jest jednak wymagana ilość miejsca do przechowywania.

Dzięki tej dodatkowej pamięci organizacje powinny uważać na wzrost kosztów i potrzeby konserwacyjne.

Jeśli wystąpi problem w źródłowym zestawie danych, taki jak uszkodzenie lub usunięcie, kopia lustrzana działa tak samo. W rezultacie dobrze jest nie polegać na kopiach lustrzanych dla wszystkich potrzeb w zakresie ochrony danych i mieć inne rodzaje kopii zapasowych danych.

Przestrzegaj zasady tworzenia kopii zapasowych 3-2-1 , która obejmuje trzy kopie danych na dwóch różnych nośnikach, z jedną kopią poza siedzibą.

Jeden określony rodzaj dublowania, dublowanie dysku, jest również nazywany RAID 1.
Ten proces replikuje dane na dwa lub więcej dysków. Dublowanie dysków jest dobrym rozwiązaniem w przypadku danych, które wymagają wysokiej dostępności ze względu na szybki czas odzyskiwania. Jest również pomocny w przypadku odzyskiwania po awarii ze względu na możliwość natychmiastowego przełączania awaryjnego. Dublowanie dysku wymaga co najmniej dwóch dysków fizycznych.
Jeśli jeden dysk twardy ulegnie awarii, organizacja może użyć kopii lustrzanej. Dublowanie dysku zapewnia wszechstronną ochronę danych, ale wymaga dużej pojemności.

Postępuj właściwie dla swojej organizacji
Organizacjom z małymi zestawami danych codzienne tworzenie pełnej kopii zapasowej zapewnia wysoki poziom ochrony bez dodatkowych kosztów związanych z przestrzenią dyskową. Większe organizacje lub te, które mają więcej danych lub woluminów serwerów, stwierdzają, że cotygodniowe tworzenie pełnej kopii zapasowej w połączeniu z codziennymi przyrostowymi lub różnicowymi kopiami zapasowymi stanowi lepszą opcję. Korzystanie z mechanizmów różnicowych zapewnia wyższy poziom ochrony danych, krótszy czas przywracania w większości scenariuszy i niewielki wzrost pojemności magazynu.
Z tego powodu stosowanie strategii cotygodniowych pełnych kopii zapasowych z codziennymi kopiami różnicowymi jest dobrą opcją dla wielu organizacji.

**Strategie backupu**

Wykonywania kopii bezpieczeństwa zawsze musi być połączone z odpowiednim zarządzaniem nośnikami, tak by w razie awarii można było szybko odtworzyć możliwie najświeższe dane, zachowując jednocześnie wymóg efektywnego wykorzystania nośników. Ze względu na wykorzystanie nośników wyróżnia się następujące metodybackup'u:
backup pojedynczy -- kopia wykonywana jest każdorazowo na tej samej pojedynczej taśmie lub zestawie taśm,
backup cykliczny -- kilka taśm lub zestawów taśm wykorzystywanych cyklicznie,
backup'y z rotacją taśm (dziś to nie zawsze taśma) -- najlepsze:
dziadek - ojciec - syn (grandfather - father - son):
wymaga 21 taśm (zestawów taśm) na rok:
4 taśmy (nazwane: poniedziałek, wtorek, środa i czwartek) przeznaczone są na backup przyrostowy lub różnicowy wykonywany każdego wieczora,
5 taśm tygodniowych przeznaczonych na pełny backup w każdy piątek,

12 taśm miesięcznych przeznaczonych na pełny backup pod koniec każdego miesiąca.
wieża Hanoi (patrz rys. [*]: ilość taśm (zestawów) wzrasta wraz czasem:
na taśmach z zestawu A wykonywany jest co drugi dzień backup przyrostowy lub różnicowy,
na taśmach z zestawu B wykonywany jest co czwarty dzień backup pełny, przyrostowy lub różnicowy,
na taśmach z zestawu C wykonywany jest co ósmy dzień backup pełny,
na taśmach z zestawu D wykonywany jest co 16 dni backup pełny,
itd.
Taśmy o najdłuższym cyklu powinny być przechowywane z dala od systemu komputerowego, najlepiej w sejfie.


**Dobre praktyki**

Przy tworzeniu wszystkich procedur związanych z robieniem kopi zapasowych danych, należy rozważyć z jednej strony możliwe ryzyko, a z drugiej koszty które trzeba będzie ponieść w związku z wprowadzeniem takiego rozwiązania. Istnieje kilka stuprocentowych metod kopiowania i zabezpieczania kopii zapasowych. Jednak te metody są niezwykle kłopotliwe w zastosowaniu. Prawdopodobnie kłopoty z ich wdrożeniem będą większe niż ostateczne zyski. Poniżej przedstawiamy kilka rozsądnych zasad, którymi warto się kierować budując strategię robienia backupu:

1. **Zaplanuj swoją strategię robienia kopii bezpieczeństwa.**

Rozpisz plan, który będzie odpowiadał na następujące pytania:

A. Co jest kopiowane do backupu?
B. Gdzie są przechowywane kopie bezpieczeństwa?
C. Jak często będą wykonywane?
D. Kto jest odpowiedzialny za wykonywanie kopii zapasowych?
E. Kto jest odpowiedzialny za sprawdzanie czy kopie bezpieczeństwa są robione właściwie i czy spełniają swoje zadanie?

2. **Pomyśl nie tylko o komputerach biurowych.**

Oczywiście należy zrobić kopie bezpieczeństwa danych znajdujących się na wszystkich biurowych komputerach, laptopach i serwerach.
Warto jednak pomyśleć również o domowych komputerach pracowniczek i pracowników.
Co z telefonami komórkowymi?
Co z kopią waszej strony internetowej?
Co z danymi, które przechowywane są w chmurze?
W jaki sposób dbacie o bezpieczeństwo wysyłanych emaili?
Zastanów się również nad bezpieczeństwem dokumentów, które są przechowywane wyłącznie w wersji papierowej. Dane w nich zawarte są bardzo trudne do odtworzenia. Chodzi to przede wszystkim o takie dokumenty jak:

A. Dokumenty finansowe
B. Informacje dotyczące osób pracujących w organizacji i z nią współpracujących
C. Umowy
D. Informacje dotyczące kredytów, pożyczek czy rat organizacji

Tego rodzaju dane powinny być przechowywane w sejfie lub dobrze zabezpieczonym archiwum, jak również należałoby przechowywać w bezpiecznym miejscu ich kopie elektroniczne (w formie oryginalnej lub skanu).

### 3. Najwyższy priorytet przyznaj kluczowym danym

Każda organizacja powinna rozważyć utratę jakiej części swojej pracy jest w stanie zaryzykować i odpowiednio do tego, zbudować swoją strategię tworzenia backupu. Najcenniejsze są zawsze bazy danych oraz dokumenty finansowe. Powinny one być zabezpieczane przed i po każdym użyciu.
W przypadku większości organizacji, oznacza to codzienne robienie ich kopii. Organizacje, które wprowadzają do systemu bardzo dużo danych, powinny rozważyć robienie backupu po każdym większym wprowadzeniu danych do systemu. Najważniejsze pliki i foldery powinny być kopiowane przynajmniej raz w tygodniu, a nawet każdego dnia.
Zazwyczaj nie stosuje się kopiowania całej zawartości twardego dysku czyjegoś komputera, szczególnie że większość tej przestrzeni zajmuje system operacyjny oraz pliki programów, które można łatwo odtworzyć z płyty.

### 4. Przechowywanie i ochrona kopii zapasowych

W przypadku przechowywania kopi bezpieczeństwa “na miejscu” można zastosować metodę zmieniania miejsca przechowywania kopii np. raz w tygodniu (miejsce przechowywania może, a nawet powinno

znajdować się poza biurem). W wersji idealnej kopie bezpieczeństwa należy przechowywać w naprawdę bezpiecznym miejscu, np. w skrzynce depozytowej. Inną metodą jest „2x2x2”, czyli dwie kopie bezpieczeństwa, przechowywane przez dwie osoby w dwóch różnych miejscach.
Szczególnie jeśli okolica, w które mieści się biuro jest podatna np. na katastrofy naturalne warto zastanowić się nad tym głębiej. Ważne, żeby mieć pewność, że zarówno dane przechowywane na miejscu, jak i te zdalne nie zostaną dotknięte przez tę samą katastrofę, która może dotknąć wasze biuro.
Jakkolwiek przesadnie mogą brzmieć te porady, warto jednak się nad nimi zastanowić. Nawet jeśli nie mieszkasz w regionie czy okolicy podatnej na katastrofy naturalne, nigdy nie wiadomo co może się wydarzyć

**5. Pomyśl o dostępie do kluczowych danych**

Jakie dane należy koniecznie mieć na wyciągnięcie ręki w razie sytuacji kryzysowej?
Jeśli padnie internet, jakie informacje, pliki, foldery są konieczne dla organizacji do pracy do czasu, kiedy internet pojawi się znowu i będzie można odzyskać dostęp do pozostałych danych?
Gdzie będziecie przechowywać te dane?

**6. Sprawdź swój backup zanim będzie naprawdę potrzebny**

Upewnij się, że zrobione kopie zapasowe można bez problemu odczytać. Ustal jak będzie wyglądał plan naprawczy i przetestuj go na różnych komputerach, tak aby sprawdzić jego skuteczność.