



Narzędzia umożliwiające tworzenie scentralizowanej polityki prowadzenia backupów

Prowadzący: prof. dr hab. inż. Mikołaj Karpiński
Opracowanie: Bogumił Gargula

Wstęp

W dzisiejszych czasach najcenniejszą rzeczą jaką posiadają Firmy, są dane. nie ma znaczenia, czy są to bazy danych klientów, czy są to dane księgowe, czy też jakiegokolwiek inne dane. W każdym przypadku ich utrata wiąże się z dotkliwą stratą dla Firmy, przestojem w działalności, a w efekcie końcowym z ogromnymi kosztami i utratą dochodu. W przypadku utraty danych medycznych, wiąże się to również z odpowiedzialnością karną, gdyż odpowiednie ustawy nakładają obowiązek przechowywania takich danych przez określony, długi okres czasu.

- Jak wykonać kopię zapasową plików i być pewnym, że dane o znaczeniu strategicznym dla przedsiębiorstwa w razie potrzeby będą zawsze dostępne?
- Jak chronić prywatność klientów?

Najważniejsze pytanie, będące zarazem odpowiedzią na powyższe zagadnienia brzmi: gdzie firmowe dane powinny być przechowywane? Czy powinny znajdować się na lokanych dyskach twardych w komputerach użytkowników/pracowników, czy na centralnym urządzeniu sieciowym - serwerze?

Dawniej ten problem praktycznie nie istniał. Obecnie nowoczesne komputery stacjonarne i notebooki dostępne są z dyskami o dużej pojemności, mogącymi pomieścić znaczne ilości danych. Nie jest problemem znaleźć komputer PC z dyskiem o pojemności większej niż 500 GB i najtańszego notebooka dysponującego dyskiem 160 GB. Z urządzeniami o tak dużej pojemności, łatwo jest o błędne przekonanie, że to właśnie na lokalnych dyskach twardych należy przechowywać wszystkie informacje. W dodatku, same systemy operacyjne Windows i Macintosh udostępniają proste metody dzielenia się zbiorami i zapewniają bezpieczeństwo w postaci loginów i haseł użytkowników. Nawet jeśli komputery i systemy operacyjne przystosowane są do składowania dużych ilości danych i gdy może wydawać się to dobrym rozwiązaniem w małych firmach, to przechowywanie ważnych informacji biznesowych na komputerach lokalnych jest obciążone pewnym ryzykiem:

- Komputery stale zagrożone są przez wirusy, które mogą uszkodzić lub zniszczyć posiadane dane.
- Komputery nie są odporne na uszkodzenia. Jeśli jedyny posiadany dysk (bo najczęściej tylko w jeden dysk wyposażonych jest większość komputerów lokalnych) ulegnie awarii, to firmowe dane, które nie są prawidłowo chronione, mogą zostać utracone. Według ostatnich badań przeprowadzonych przez Google, średnio 1.7% twardych dysków ulega awarii w ciągu roku i ponad 8.6% w przeciągu trzech lat.
- Komputery służbowe znajdujące się w biurach są najczęściej źle zabezpieczone fizycznie. Znający się na rzeczy intruz może je z łatwością odnaleźć i uszkodzić. Oprócz tego, fizycznie źle zabezpieczone komputery (stacjonarne lub laptopy), mogą zostać skradzione.
- Istnieje duże prawdopodobieństwo, że laptopy (na których często znajdują się ważne informacje firmowe) użytkowane przez pracowników będących często w podróży służbowych, mogą zostać zagubione lub skradzione. Z najnowszych badań Ponemon Institute, sponsorowanych przez firmę Dell wynika, że do 12000 notebooków jest traconych co tydzień na lotniskach. Pięćdziesiąt trzy procent ankietowanych

podróżujących służbowo oznajmiło, że przewożą poufne informacje firmowe, ale - co zaskakujące 42% respondentów przyznało, że nie robi kopii zapasowych swoich danych. Badania pokazują również, że od 65% do 70% utraconych notebooków nie jest zgłaszanych.

Aby uchronić firmowe dane przed powyższymi zagrożeniami, małe przedsiębiorstwa powinny opracować politykę scentralizowanego gromadzenia danych, czyli politykę gromadzenia danych na serwerach. Oto korzyści takiego rozwiązania:

- Wszystkie dane przedsiębiorstwa mogą być przechowywane na wspólnym urządzeniu, na którym dzięki oprogramowaniu można wykonywać kopie zapasowe.
- Pliki przechowywane na serwerze mogą być udostępniane indywidualnym użytkownikom lub całym grupom użytkowników oraz mogą pozostać poufne dla innych. To rozwiązanie eliminuje również efekt „sneakernet”, polegający na potrzebie wymiany/przenoszenia plików na nośnikach zewnętrznych (np. pamięciach USB, dyskietkach, taśmach magnetycznych, dyskach twardych).
- Z ekonomicznego punktu widzenia, dobrą inwestycją jest zakup nieulegającego awariom urządzenia, służącego do przechowywania danych. Odporność na awarie polega na zastosowaniu opcji RAID, jak również uniknięciu przerw w dostawie zasilania (dzięki dodatkowemu urządzeniu UPS). Dla większości przedsiębiorstw nie opłacalne jest budowanie systemu odpornego na awarie osobno dla każdego komputera w firmie.
- Przed uszkodzeniem fizycznym łatwiej jest zabezpieczyć serwer, niż wszystkie używane w firmie komputery.
- Znacznie prostsza jest polityka zarządzania dostępem do danych, gdy wszystkie informacje zgromadzone są w na jednym centralnym serwerze. Gdy w sieci P2P (peer-to-peer) liczba komputerów przekroczy cztery lub pięć, to zarządzanie „rozproszonymi” danymi, przechowywanymi na tych komputerach szybko stanie się niemożliwe.
- Zgromadzenie wszystkich firmowych danych do jednej centralnej lokalizacji, powoduje optymalizację wydatków przedsiębiorstwa w aspekcie przechowywania danych. Pieniądze zainwestowane w zakup serwera, mogą przynajmniej częściowo zwrócić się przez zakup standardowych komputerów z minimalnymi wymaganiami technicznymi – w tym z dyskami o mniejszej pojemności. Oprócz tego, możliwe będzie efektywniejsze wykorzystanie dostępnej pojemności twardych dysków w komputerach, gdyż nie będą one potrzebne do gromadzenia danych.

Strategia polegająca na scentralizowanym przechowywaniu danych obejmuje przede wszystkim wybór odpowiedniego urządzenia, czyli centralnej platformy pamięci masowej. Zasadniczo istnieją dwie możliwości: PC z systemem operacyjnym Microsoft Windows Serwer lub dysk sieciowy NAS, taki jak np. Synology, QNAP, Buffalo czy CTERA. Obie platformy pamięci masowej zapewniają korzyści płynące z scentralizowanego przechowywania danych, ale każdy prezentuje swoje wady i zalety.

Niektóre aplikacje, takie jak np. Microsoft Exchange Server oraz niektóre aplikacje baz danych, muszą działać na systemie Microsoft. Aplikacje te wymagają dostępu blokowego do dysku. W najprostszej formie znajdują się one na urządzeniach typu DAS, czyli bezpośrednio podłączonych nośnikach pamięci (np. pamięć flash USB). Wdrażanie systemu przechowywania danych opartego na Windowsie

zwykle wymaga także zaangażowania specjalistów z branży IT. Dla wielu małych przedsiębiorstw, nie mogących pozwolić sobie na zatrudnienie pełnoetatowych pracowników, pozostaje zlecenie takiej usługi zewnętrznej firmie, która odpłatnie wdraża System i jest odpowiedzialna za jego utrzymywanie. Serwery te wymagają również regularnych uaktualnień Microsoftu, jak i zainstalowania programu antywirusowego, co prowadzi do dalszego wzrostu kosztów posiadania takiego rozwiązania.

Wiele małych przedsiębiorstw nie potrzebuje aplikacji takich jak np. baza danych, czy serwer poczty, gromadzonych na serwerze. Często ich wiadomości email obsługiwane są przez zewnętrznego dostawcę usługi (operatora) lub przez operatora poczty POP (protokół internetowy, pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera), takiego jak Google. Dla takich przedsiębiorstw, serwer NAS mógłby być idealnym elementem strategii centralnego gromadzenia danych. Każdy serwer NAS zapewnia wszystkie korzyści płynące z centralnego przechowywania danych, ale ma też wiele zalet w stosunku do konwencjonalnych serwerów opartych na systemie Windows:

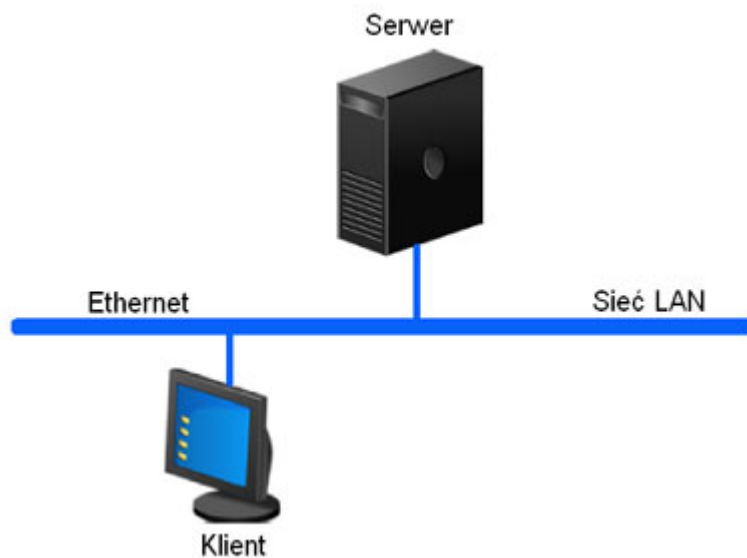
- Większość serwerów plików odporne są na awarie dzięki technologii RAID. W zależności od konfiguracji RAID, dane zostaną zachowane nawet jeśli dojdzie do awarii jednego lub kilku dysków w macierzy. Dodatkowo funkcja Hot Swap umożliwia odłączenie i wymianę uszkodzonego dysku, bez konieczności wyłączenia urządzenia. Eliminuje to jakiegokolwiek przestoje w pracy serwera.
- System operacyjny Linux, na którym opierają się serwery, ma kilka podstawowych zalet:
 - jest bardzo prosty do skonfigurowania dla osób nie będących specjalistami z branży IT. Przyjazny interfejs użytkownika oraz prosty kreator instalacji powodują, że pełne uruchomienie urządzenia zabiera około 15 minut.
 - Dodatkowa pojemność do magazynowania danych może być dodana do istniejącej już sieci, poprzez zainstalowania serwera. Od momentu podłączenia urządzenia do istniejącej sieci Ethernet, nie będzie żadnych przestojów w pracy serwera, jak to ma miejsce w serwerach bazujących na systemie Windows.
 - Serwery łatwo integrują się z istniejącym środowiskiem sieciowym.
 - Dzięki wbudowanej usłudze Active Directory, można być łatwo skonfigurowany jako urządzenie magazynujące w istniejącej sieci Windows.
 - Serwery opierają się na technologii iSCSI, wykorzystującej protokół TCP/IP do połączenia z serwerem. Klienci, w tym serwery używając oprogramowania iSCSI Inicjator, mogą połączyć się z targetem iSCSI i mieć dostęp na poziomie blokowym do zgromadzonych danych. Target iSCSI będzie widoczny jako dysk lokalny na komputerze użytkownika, który podłączył udział iSCSI. Aplikacja wymagająca dostępu do dysku na poziomie blokowym, tak jak niektóre bazy danych lub aplikacje email, mogą wykorzystywać target iSCSI zamiast bezpośrednio podłączanych nośników pamięci DAS.
 - Praktycznie wszystkie serwery NAS zapewniają wsparcie użytkownikom takich platform jak: Windows, Macintosh i

Linux/Unix. Nie wymagana jest przy tym żadna specjalna konfiguracja.

- Linux jest stabilnym systemem operacyjnym, który rzadko wymaga poprawek.
- Nie ma opłat licencyjnych, co powoduje brak dodatkowych kosztów.
- Wirusy i inne złośliwe oprogramowania bardzo rzadko atakują.

Dla małych i średnich przedsiębiorstw, przechowywanie danych na serwerach oferuje więcej zalet w odniesieniu do gromadzenia na dyskach lokalnych. W porównaniu do archiwizacji bazujących na systemach Windows, rozwiązania serwerów NAS są dużo rozsądniejszymi alternatywami.

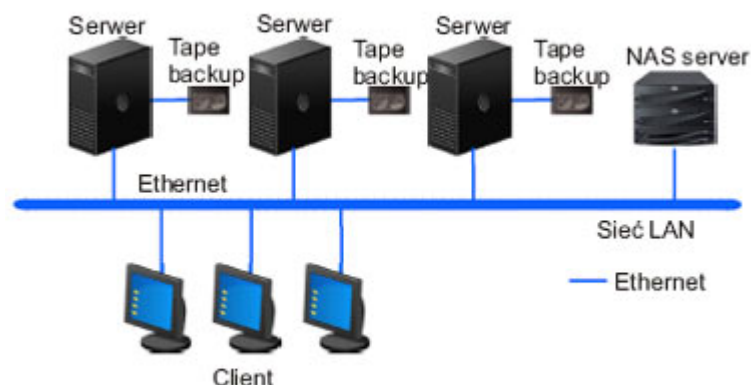
Client/Server



To najprostsza konfiguracja pamięci masowej często w przypadku bardzo małych firm. Podpięty do sieci użytkownik zapisuje dane albo na swoim własnym komputerze albo poprzez sieć LAN na serwerze plików. Zapewnia to użytkownikowi podstawową ochronę ważnych plików, ale poza najprostszymi zastosowaniami nie daje żadnych dodatkowych funkcjonalności.

Ponieważ koszty związane z utratą danych są ogromne, dlatego też coraz więcej firm decyduje się na wdrożenie kompletnego systemu ochrony danych. W tym celu niezbędne jest przygotowanie infrastruktury pamięci masowych, używanej do składowania informacji. W zależności od wymagań związanych z wydajnością, niezawodnością czy skalowalnością, użytkownik ma do wyboru trzy możliwości: DAS, NAS lub SAN.

DAS (Direct Attached Storage)



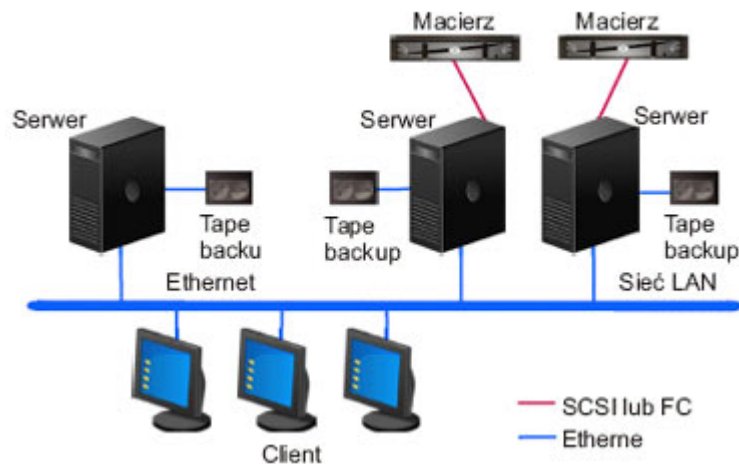
DAS jest rozwiązaniem, w którym każdy serwer posiada dedykowaną pamięć masową podłączoną bezpośrednio poprzez interfejs SCSI lub FC. Operacje odczytu/zapisu związane m.in. z kopiami bezpieczeństwa, odtworzeniami czy archiwizacją przeprowadzane są bezpośrednio na podłączony zasób. Zasób ten nie jest współdzielony a dostęp do niego posiada tylko serwer do którego jest on podpięty.

Zaletą topologii DAS jest łatwość implementacji oraz wysoka wydajność ze względu na fakt, iż każdy serwer posiada dedykowany zasób. Wadami rozwiązania DAS są: słaba skalowalność, brak możliwości centralnego, efektywnego zarządzania, wysokie koszty implementacji w przeliczeniu na pojedynczy serwer, niska niezawodność.

Rozwiązanie DAS może być stosowane w przypadku, gdy chcemy zbudować infrastrukturę złożoną z kilku serwerów o ściśle zdefiniowanej, wymaganej pojemności pamięci masowej i nie planujemy jej dalszej rozbudowy w przyszłości.

DAS jest jednym z pierwszych rozwiązań na rynku pamięci masowych i od dłuższego czasu zastępowany rozwiązaniami typu NAS czy SAN.

NAS (Network Attached Storage)



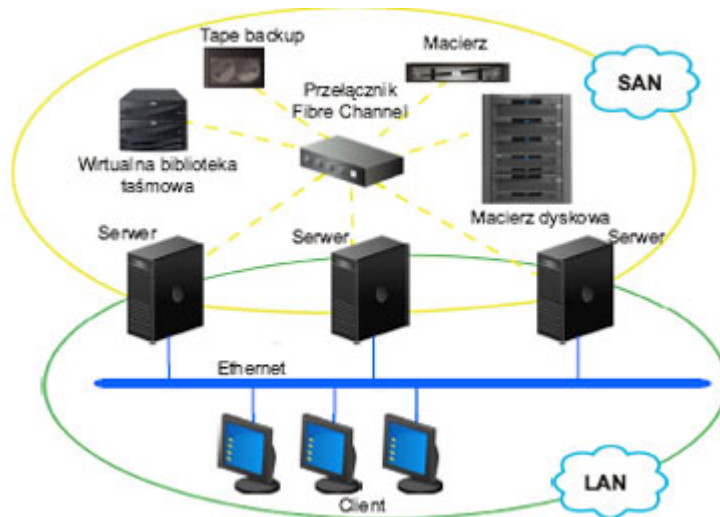
NAS to rozwiązanie, w którym dedykowany serwer NAS udostępnia zasoby pamięci masowych poprzez sieć IP z wykorzystaniem protokołów NFS, CIFS, AppleTalk.

NAS jest rozwiązaniem efektywnym ekonomicznie ze względu na centralizację zasobów pamięci masowych udostępnianych wielu serwerom, a zasoby są podpięte bezpośrednio do serwera NAS, poprzez interfejs FC lub SCSI. Udostępnianie zasobów poprzez sieć IP umożliwia zazwyczaj wykorzystanie istniejącej infrastruktury sieciowej i co za tym idzie zwrot poniesionych nakładów (ROI). Centralizacja zmniejsza koszty związane z zarządzaniem, diagnostyką i pozwala efektywnie wykorzystać posiadane zasoby. Poprzez NAS można współdzielić dane w heterogenicznych środowiskach systemowych.

Wadami NAS są: słaba wydajność związana ze współdzieleniem dostępu do danych poprzez centralny punkt (serwer NAS), ograniczona skalowalność związana z rozbudową pamięci masowych, wydajność ograniczona sposobem dostępu do danych.

Rozwiązanie NAS można stosować w przypadku, gdy chcemy zbudować infrastrukturę, w której satysfakcjonujący jest dostęp na poziomie plikowym, wydajność oraz niezawodność nie są krytycznymi parametrami, natomiast zależy nam ekonomicznej implementacji rozwiązania umożliwiającego współdzielony dostęp do zasobów pamięci masowych w środowisku heterogenicznym, z wykorzystaniem sieci IP. Obecnie małe firmy i instytucje bardzo często korzystają z prostych rozwiązań typu NAS do skutecznego przechowania danych w postaci plikowej.

SAN (Storage Area Network)



SAN jest rozwiązaniem, w którym głównym elementem składowym jest przełącznik za pośrednictwem którego serwery uzyskują dostęp do pamięci masowych. Sieć SAN można zbudować z wykorzystaniem protokołu Fibre Channel (FC SAN) lub iSCSI (IP SAN). Wszystkie elementy składowe takie jak serwery czy pamięci masowe są podłączone za pośrednictwem przełącznika lub przełączników. Dzięki centralizacji oraz wielu ścieżkom dostępu do danych otrzymujemy rozwiązanie wysoce niezawodne oraz niezwykle wydajne, przy jednoczesnej możliwości kompleksowego zarządzania całą infrastrukturą. Ze względu na pełną modułowość, sieć SAN jest efektywnie skalowalna. Wadą rozwiązania sieci SAN są wysokie koszty implementacji (FC SAN), które jednak można znacząco zmniejszyć opierając budowę całej infrastruktury na protokole iSCSI (IP SAN).

Rozwiązanie SAN można stosować w przypadku, gdy chcemy zbudować infrastrukturę, w której krytycznymi parametrami są niezawodność oraz wydajność, bez ograniczeń związanych z liczbą zainstalowanych serwerów oraz pamięci masowych, z możliwością efektywnej rozbudowy.

Poniżej podsumowanie wspomnianych architektur systemów pamięci masowej:

parametr	DAS	NAS	SAN	
			FC SAN	IP SAN
Koszt dodania nowego serwera	wysoki (zakup dedykowanej pamięci masowej oraz kontrolera)	niski (podłączenie serwera do sieci IP),	wysoki (zakup dedykowanej karty HBA)	niski (podłączenie serwera do sieci IP).
Koszt infrastruktury	brak dedykowanej infrastruktury (każdy serwer podłączony bezpośrednio do pamięci masowej)	niski (możliwość wykorzystania dostępnej infrastruktury IP)	Wysoki (budowa niezależnej infrastruktury FC, przełącznik FC, karty HBA)	Niski (możliwość wykorzystania dostępnej infrastruktury IP plus dedykowany przełącznik iSCSI).
Wymagane umiejętności	znajomość urządzeń SCSI lub FC	znajomość mechanizmów sieci IP	znajomość mechanizmów sieci FC	znajomość mechanizmów sieci IP
Zdalne współdzielenie zasobów	Brak	IP - poprzez LAN, MAN, WAN	kosztowne - z wykorzystaniem protokołów IFCP lub FCIP	IP - poprzez LAN, MAN, WAN
Niezawodność	Niska	Średnia	Wysoka	Wysoka
Wydajność	Wysoka	Niska - dostęp poprzez centralny punkt wspólny (serwer NAS)	Wysoka	Średnia
Skalowalność	Niska	Średnia	Wysoka	Wysoka

Rodzaje backupów

Backup całościowy (*full backup*)

Procesowi backupu całościowego podlegają wszystkie dane, bit „archive” plików jest ustawiany w stan „0”.

Zalety:

- łatwość wyszukiwania dowolnych danych (*wszystkie znajdują się na jednym nośniku*)
- Odtworzenie systemu można przeprowadzić bardzo szybko

Wady:

- Nieefektywne wykorzystanie nośników - cały czas są backupowane dane rzadko ulegające zmianom
- Długi czas wykonywania operacji
-

Backup przyrostowy (*incremental backup*)

Zapisywane są tylko te dane, które powstały lub uległy zmianie od czasu przeprowadzenia ostatniego całościowego lub przyrostowego backupu; backupowane są pliki, które bit „archive” mają ustawione w stan „1”, a po tej operacji bit „archive” jest przestawiany w stan „0”.

Zalety:

- Czas przeprowadzenia backupu jest bardzo krótki
- Efektywne wykorzystanie nośników

Wady:

- Trudność wyszukiwania danych (*do odnalezienia zbioru są potrzebne wszystkie nośniki z backupami przyrostowymi oraz ostatni nośnik z backupem całościowym*)
- Długi czas odtworzenia systemu
-

Backup różnicowy (*differential backup*)

Zapisywane są tylko te dane, które uległy zmianie od czasu przeprowadzenia ostatniego całościowego lub przyrostowego backupu; backupowane są pliki, które bit „archive” mają ustawione w stan „1”. Po tej operacji nie ulega on zmianie.

Zalety:

- łatwy sposób wyszukiwania dowolnych danych (*do odnalezienia dowolnego zbioru potrzebne są maksymalnie dwa nośniki*)
- Odtworzenie systemu przeprowadza się stosunkowo szybko
- Czas przeprowadzenia backupu dużo krótszy niż w przypadku backupu całościowego
-

Wady:

- Nieefektywne wykorzystanie nośników; nadmiarowość backupów, dane które nie uległy zmianie, są cały czas backupowane
- Dłuższy czas wykonywania operacji niż backupów przyrostowych
-

Backup lokalny**Zalety:**

- Prosta instalacja i konfiguracja
- Szybki transfer danych
- Krótki czas konieczny do wykonania backupu

Wady:

- Konieczna regularna (często *codzienna*) ingerencja człowieka
- Duże ryzyko wystąpienia tzw. błędu ludzkiego
- Szybki wzrost kosztów (*sprzętu, oprogramowania, administracji*)
- Utrudniona automatyzacja
-

Backup sieciowy**Zalety:**

- Centralne zarządzanie
- Prosta „naturalna” automatyzacja
- Niskie koszty administracji

Wady:

- Bardzo duże obciążenie sieci
- Wolny transfer danych
- Stosunkowo długi czas konieczny do wykonania backupu
- Słabe wykorzystanie możliwości sprzętu

Kopia zapasowa w Windows 7

Funkcja wykonywania kopii zapasowych i przywracania, ulepszona w systemie Windows 7, umożliwia wykonywanie kopii bezpieczeństwa najważniejszych plików osobistych, dzięki czemu można być zawsze przygotowanym na najgorsze.

Można zezwolić systemowi Windows na wybranie plików, które mają zostać uwzględnione w kopii zapasowej, lub samodzielnie wybrać poszczególne foldery, biblioteki i dyski. System Windows może wykonać kopie zapasowe w dowolnie wybranym czasie - wystarczy jedynie skonfigurować harmonogram.

Kopię zapasową można utworzyć na innym dysku lub na płycie DVD. A jeśli korzysta się z wersji Professional lub Ultimate systemu Windows 7, kopię zapasową plików można utworzyć za pośrednictwem sieci.

Tworzenie kopii zapasowej lub przywracanie plików użytkownika

Kopia zapasowa

Program Kopia zapasowa systemu Windows nie został skonfigurowany.

 [Konfiguruj tworzenie kopii zapasowej](#)

Przywróć

System Windows nie może odnaleźć kopii zapasowej tego komputera.

 [Wybierz inną kopię zapasową, aby przywrócić z niej pliki](#)

[Odzyskaj ustawienia systemu na tym komputerze](#)

1. Otwórz Panel sterowania i kliknij Wykonaj kopię zapasową komputera w sekcji System i zabezpieczenia (w widoku klasycznym Kopia zapasowa/Przywracanie).

Podczas pierwszego uruchomienia wybierz Konfiguruj tworzenie kopii zapasowej (rys.1).

Zapisz kopię zapasową w:

Miejsce docelowe kopii zapasowej	Wolne miejsce	Całkowity rozmiar
 Nowy (D:)	309,76 GB	319,28 GB
 Stacja dysków DVD RW (E:)		

Odśwież

Zapisz w sieci...



Ten dysk znajduje się na tym samym dysku fizycznym co dysk systemowy. [Wiecej informacji](#)

2. Wybierz lokalizację, w której zostanie umieszczony plik kopii (rys.2).

Możesz wskazać inną partycję, drugi dysk fizyczny, nośnik zewnętrzny (pamięć flash bądź płytę DVD), a nawet lokalizację sieciową.

Najszybszą metodą zapisu będzie wybranie dysku lub partycji ale pamiętaj, że w razie awarii nośnika dane mogą zostać utracone.

Kliknij przycisk Dalej.

Kopia w sieci

Lokalizacja sieciowa:

Przeglądaj...

Przykład: \\serwer\udział

Poświadczenia sieci

Program Kopia zapasowa systemu Windows wymaga nazwy użytkownika i hasła w celu uzyskania dostępu do lokalizacji sieciowej podczas zapisywania kopii zapasowej. [Które poświadczenia należy wprowadzić?](#)

Nazwa
użytkownika:

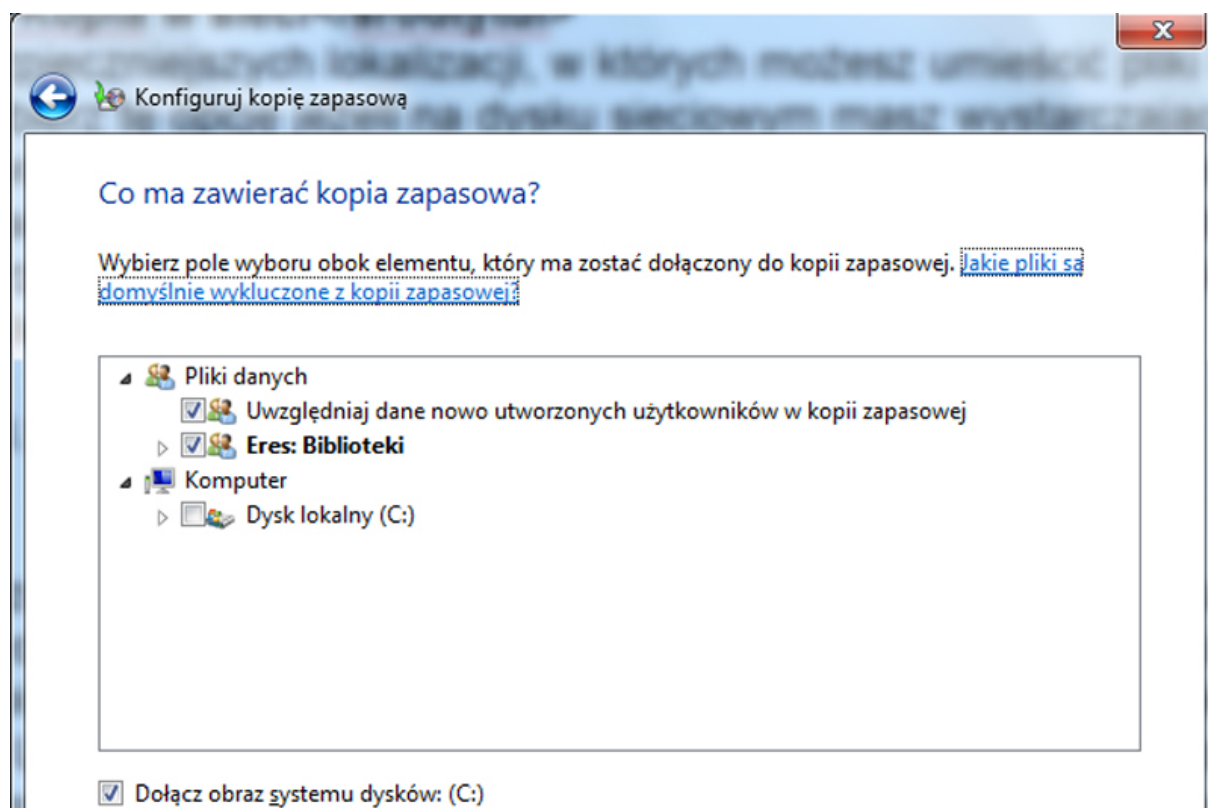
Hasło:

Jedną z bezpieczniejszych lokalizacji, w których możesz umieścić pliki kopii jest sieć lokalna. Wybierz tę opcję jeżeli na dysku sieciowym masz wystarczającą ilość miejsca a twoje uprawnienia zezwalają ci na zapis.

Kliknij Zapisz w sieci..., wpisz ścieżkę do serwera i udziału sieciowego bądź wyszukaj odpowiedni katalog po kliknięciu Przeglądaj.

Uzupełnij pola nazwą użytkownika oraz hasłem, które uprawnia do zapisu danych w sieci (rys.3).

Zaakceptuj zmiany przyciskiem OK.



3. Jeżeli pozostawisz zaznaczoną opcję Wybierz automatycznie (zalecane) Windows sam zdecyduje jakie dane zarchiwizować.

Będą to między innymi pliki z Bibliotek (tylko te zapisane lokalnie), a także z folderów Application Data, Kontakty, Pulpit, Pobieranie, Ulubione, Łącza oraz, Zapisane gry i Wyszukiwania.

Jednocześnie utworzony zostanie obraz systemu. Po kliknięciu Pozwól mi wybrać będziesz musiał sam wskazać pliki i katalogi do skopiowania (rys.4).

Uwaga! W każdym przypadku dysk źródłowy oraz docelowy muszą być sformatowane w systemie plików NTFS.

Kliknij Dalej.

☒ **Uruchamiaj wykonywanie kopii zapasowej zgodnie z harmonogramem (zalecane)**

Jak często:

Cotygodniowo

Którego dnia:

niedziela

O której godzinie:

19:00

4. W ostatnim oknie kreatora konfiguracji możesz ustalić kiedy ma być tworzona kopia zapasowa danych i jak często (rys.5).

Harmonogram zmienia się po kliknięciu łącza Harmonogram zadań.

Pamiętaj, że w czasie kiedy zaplanowany jest zapis kopii komputer powinien być łączony.

Zakończ konfigurację przyciskiem Zapisz ustawienia i uruchom wykonywanie kopii zapasowej.

Tworzenie kopii zapasowej lub przywracanie plików użytkownika

Kopia zapasowa

Lokalizacja:

Nowy (D:)



308,79 GB wolnych z 319,28 GB

Rozmiar kopii zapasowej: 954,04 MB

[Zarządzaj miejscem](#)



[Utwórz kopię zapasową teraz](#)

Następna kopia
zapasowa:

2010-05-09 19:00

Ostatnia kopia
zapasowa:

2010-05-05 12:42

Zawartość:

Pliki w bibliotekach i folderach osobistych
wszystkich użytkowników

Harmonogram:

Zawsze w tym dniu: niedziela o godzinie 19:00



[Zmień ustawienia](#)

5. Jeżeli chciałbyś wykonać pozaplanową archiwizację danych, to po uruchomieniu narzędzia Kopia zapasowa kliknij przycisk Utwórz kopię zapasową teraz (rys.6).

Możesz też zapisać sam obraz. Wybierz w tym celu łącze Utwórz obraz systemu widoczne w lewej części okna.

Odzyskiwanie danych

Przywróć

Można przywrócić pliki, których kopie zapasowe zostały utworzone w bieżącej lokalizacji.

 [Przywróć pliki wszystkich użytkowników](#)

 [Wybierz inną kopię zapasową, aby przywrócić z niej pliki](#)

Przywróć moje pliki

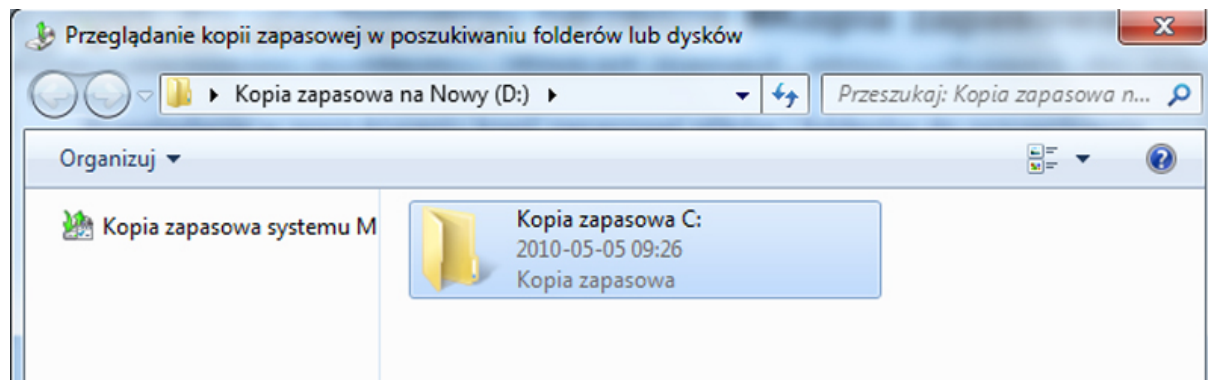
[Odzyskaj ustawienia systemu na tym komputerze](#)

1. Uruchom program Kopia zapasowa i przejdź do dolnej części okna.

Masz możliwość odzyskania swoich plików, plików innych użytkowników bądź ustawień systemu (korzysta z Punktów przywracania).

Zmianę wersji kopii wykonuje się po kliknięciu Wybierz inną kopię zapasową, aby przywrócić z niej pliki.

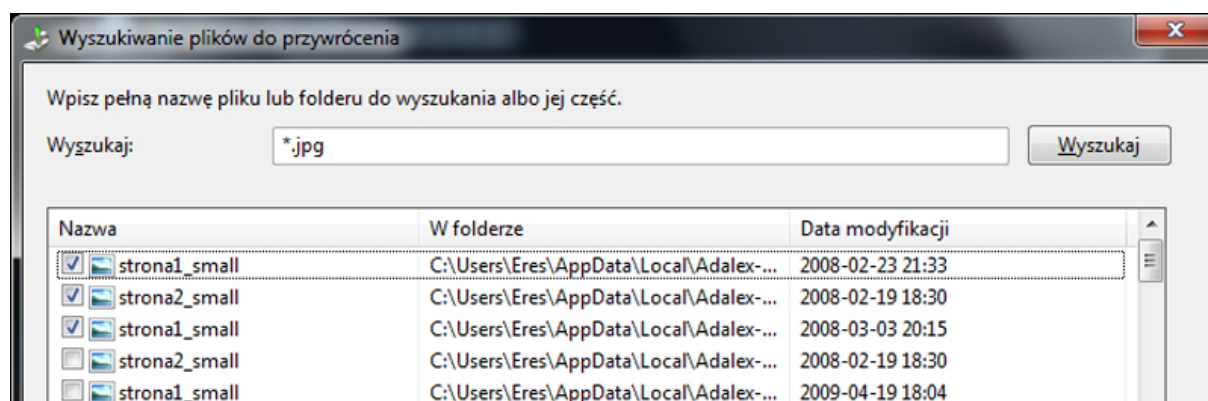
Wybierz na przykład Przywróć pliki wszystkich użytkowników (rys.7).



2. Musisz teraz określić, co chcesz odzyskać. Do wyboru masz pojedyncze pliki i całe katalogi.

Aby przywrócić wszystkie dane kliknij przycisk Przeglądaj foldery, zaznacz folder kopii zapasowej (rys.8) i kliknij Dodaj folder.

Wybierz Dalej, pozostaw domyślne zaznaczenie W oryginalnej lokalizacji i rozpocznij operację przyciskiem Przywróć.



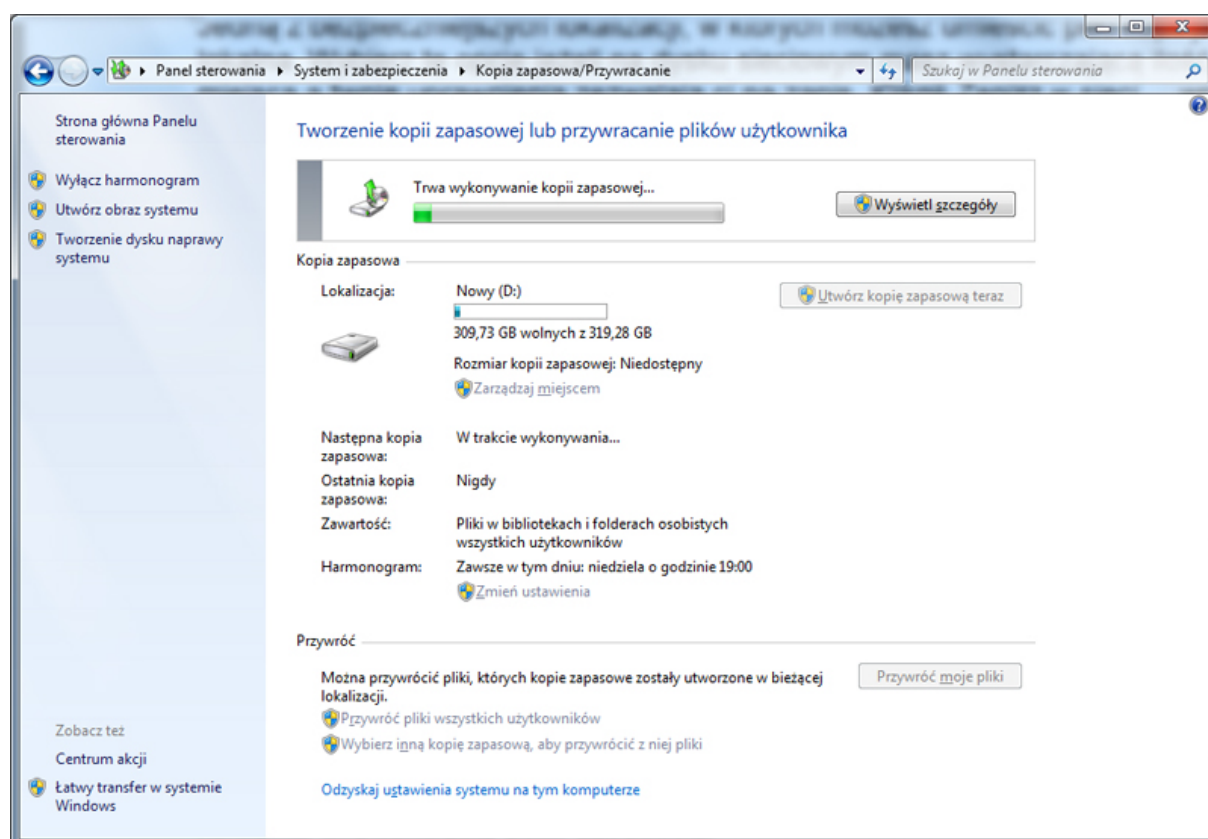
3. Pojedyncze obiekty można wyszukać po kliknięciu Przeglądaj pliki.

Pomiędzy danymi w oknie kopii porusza się tak, jak w oknie Exploratora Windows.

Możesz też skorzystać z wyszukiwarki. Wybierz w tym celu Wyszukaj...

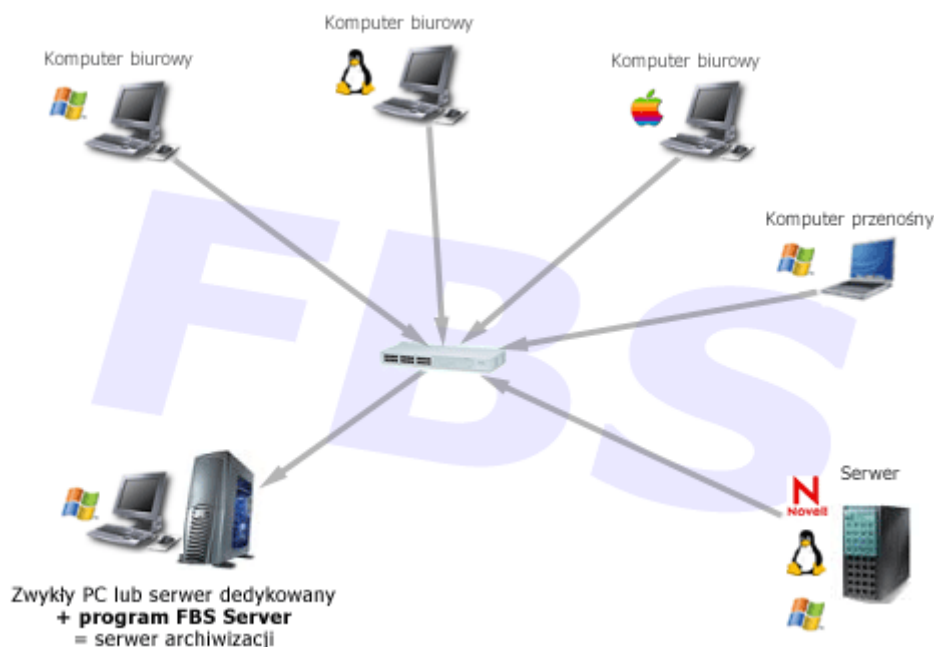
Wpisz poszukiwaną frazę i kliknij Wyszukaj. Zaznacz pliki do odzyskania i zatwierdź przyciskiem OK (rys.9).

Kliknij Dalej i Przywróć.



Program do backupu i archiwizacji komputerów w sieciach LAN

Ferro Backup System™ (FBS) to profesjonalny, sieciowy system backupu i archiwizacji danych przeznaczony dla firm i instytucji. Pozwala chronić dane przechowywane na stacjach roboczych, laptopach i sieciowych serwerach plików pracujących pod systemami Microsoft Windows®, Novell NetWare®, Linux, MacOS.



Archiwizacja danych i backup systemu wszystkich komputerów podłączonych do sieci lokalnej

Dzięki **Ferro Backup System™** w kilka chwil wykonasz backup plików lub całego systemu operacyjnego i zabezpieczysz krytyczne dla funkcjonowania Twojego przedsiębiorstwa informacje przechowywane na komputerach podłączonych do sieci lokalnej.

Szybki, równoległy backup

Ze względu na zastosowanie backupu delta i backupu różnicowego, kompresji po stronie stacji roboczych i równoległego wykonywania zadań, Ferro Backup System pozwala w bardzo krótkim czasie wykonać kopie zapasowe plików z wszystkich komputerów podłączonych do sieci lokalnej.

Niskie koszty wdrożenia rozwiązania

Ferro Backup System nie wymaga drogiego serwera, serwerowej wersji systemu operacyjnego, czy też napędów taśmowych. Ze względu na to, że backup danych odbywa się już po stronie stacji roboczych a nie na serwerze, na serwer backupu można przeznaczyć zwykły, tani komputer PC z większym dyskiem twardym.

Automatyczne wznowianie backupu

Bezobsługowość

Opcja automatycznego zwalniania miejsca na dysku w połączeniu z modulem alertów, który wysyła do administratora informacje o ewentualnych błędach i ostrzeżeniach za pomocą wiadomości e-mail, ogranicza konieczność stałego nadzoru nad procesem wykonywania backupu.

Transparentny backup

Backup jest wykonywany w tle i nie jest zauważalny dla pracowników. Administrator ustala szybkość backupu.

Wygodny backup i odzyskiwanie danych

Administrator nie musi zaprzętać sobie głowy tym, kiedy była robiona ostatnia archiwizacja pełna, a kiedy i ile zostało wykonanych archiwizacji różnicowych. Ferro Backup System przejmuje kontrolę nad procesem odzyskiwania danych z kopii różnicowych i wyświetla ich

W przypadku zerwania połączenia, zadania backupu zostaną wstrzymane i dokończone po ponownym nawiązaniu połączenia bez konieczności interwencji ze strony administratora.

Łatwa instalacja i uruchomienie

Aby wykonywać backup dysków, plików lub kopie zapasowe systemu operacyjnego, nie trzeba zmieniać niczego w aktualnej konfiguracji sieci komputerowej, serwerów i komputerów biurowych. Ferro Backup System działa całkowicie niezależnie od istniejących usług, konfiguracji kont i zabezpieczeń.

zawartość tak samo jak w przypadku kopii pełnych.

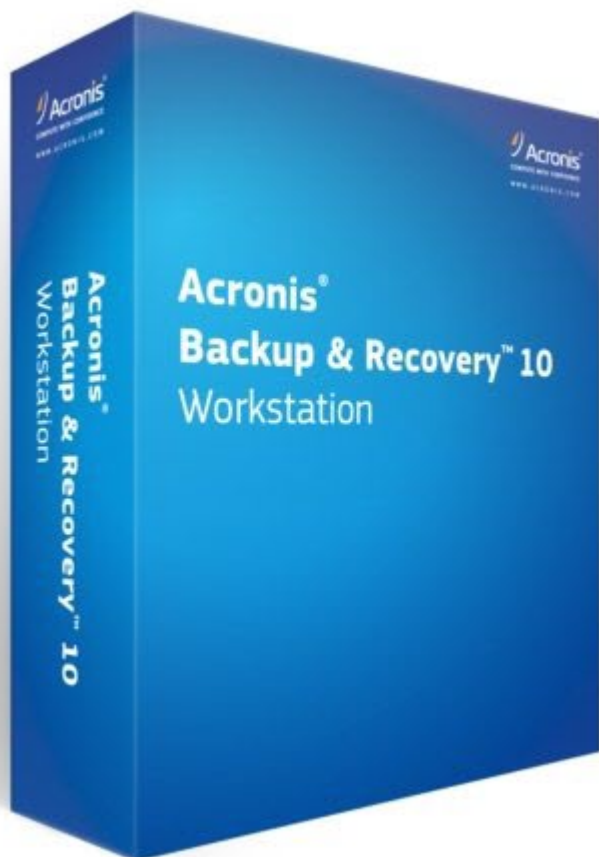
Backup otwartych plików

Wbudowana w Ferro Backup System opcja Open File Manager pozwala na backup otwartych plików systemowych oraz plików zablokowanych przez inne procesy.

Backup systemu operacyjnego

Ferro Backup System daje możliwość wykonania kopii zapasowej systemu operacyjnego oraz późniejszego przywrócenie systemu i programów na nowym, czystym dysku bez potrzeby ponownej instalacji.

Acronis® Backup & Recovery™ 10 Advanced Server



Program Acronis® Backup & Recovery™ 10 Advanced Server, oparty na opatentowanych przez firmę Acronis technologiach tworzenia obrazów dysku i przywracania systemu od podstaw, stanowi nową generację produktów Acronis True Image do odzyskiwania danych po awarii, przeznaczoną do środowisk fizycznych i wirtualnych. Program ten upraszcza i automatyzuje tworzenie kopii zapasowych i przywracanie danych w środowiskach Windows i Linux oraz umożliwia zdalne monitorowanie i zarządzanie geograficznie rozproszonymi serwerami i stacjami roboczymi. Dzięki programowi Acronis Backup & Recovery 10 Advanced Server czas odzyskiwania systemu operacyjnego, aplikacji i wszystkich danych liczy się w minutach, a nie w godzinach lub dniach.

Ponieważ program Acronis Backup & Recovery 10 Advanced Server opracowano dla przedsiębiorstw różnej wielkości, można go rozbudować do obsługi tysięcy komputerów. Dzięki niemu firma uzyskuje dostęp do zaawansowanych funkcji tworzenia kopii zapasowych i odzyskiwania systemu, takich jak: deduplikacja danych, udoskonalone zabezpieczenia, operacyjny pulpit roboczy i zarządzanie na podstawie zasad itp.

Wykorzystując wydajność i wyjątkową łatwość obsługi programu Acronis Backup & Recovery 10 Advanced Server, przedsiębiorstwo może uprościć stosowane procesy tworzenia kopii zapasowych i odzyskiwania danych oraz spełnić bardziej rygorystyczne wymagania dotyczące docelowego czasu odtwarzania (RTO). Ponadto firma Acronis oferuje kilka narzędzi opcjonalnych, za pomocą których można dodatkowo zwiększyć funkcjonalność programu Acronis Backup & Recovery 10 .

- Opcjonalne narzędzie Acronis® Backup & Recovery™ 10 Deduplication zwiększa atuty wynikające z tworzenia międzydyskowych kopii zapasowych serwerów, ponieważ zmniejsza ilość nadmiarowych danych uwzględnianych w kopiach zapasowych, dzięki czemu obniża koszt przechowywania danych i umożliwia optymalne wykorzystanie pojemności pamięci masowej.
- Dodatkowo, korzystając z opcjonalnego narzędzia Acronis® Backup & Recovery™ 10 Universal Restore™, administrator może szybko zautomatyzować proces odzyskiwania nawet w przypadku wykonywania go na innym sprzęcie lub na maszynie wirtualnej.

Program Acronis Backup & Recovery 10 Advanced Server współpracuje z komputerami fizycznymi i maszynami wirtualnymi dzięki wykorzystaniu agentów. Jeśli potrzebne są dodatkowe sposoby tworzenia kopii zapasowych i przywracania hostów wirtualnych, to Acronis® Backup & Recovery™ 10 Advanced Server Virtual Edition oferuje bardziej kompleksowe metody tworzenia kopii zapasowych serwera — nie wykorzystujące agentów i oparte na hoście — zarówno dla hosta, jak i wielu maszyn wirtualnych.

Główne korzyści

- **Ograniczenie przestoju i krótki czas odzyskiwania danych**

Całą zawartość dysku twardego — w tym system operacyjny, aplikacje i dane — można odzyskać w ciągu kilku minut, a nie godzin lub dni.

- **Scentralizowane zarządzanie i poprawa wydajności działu IT**

Procesy tworzenia kopii zapasowych i odzyskiwania danych obejmujące wszystkie stacje robocze i serwery są wykonywane w jednym miejscu sieci — program zawiera scentralizowany pulpit roboczy z przeglądem operacji skonfigurowanych i wykonywanych we wszystkich systemach, zapewniając większą kontrolę i usprawniając podejmowanie decyzji.

- **Oszczędność pamięci masowej i przepustowości sieci dzięki deduplikacji danych**

Opcjonalne narzędzie Acronis® Backup & Recovery™ 10 Deduplication oferuje przystępne funkcje programowej deduplikacji na poziomie plików i bloków, umożliwiając przedsiębiorstwu różnej wielkości lepsze wykorzystanie infrastruktury pamięci masowej i obniżenie kosztów.

- **Automatyzacja odzyskiwania przy użyciu prostego procesu ze wskazówkami**

Intuicyjny w obsłudze interfejs ułatwia instalację, przyspiesza konfigurację i wdrożenie programu oraz upraszcza korzystanie z niego zarówno w przypadku doświadczonych informatyków, jak i początkujących użytkowników.

- **Uwolnienie działu IT od powtarzalnych zadań**

Dzięki funkcji grupowania zasady i procedury można zastosować w określonej grupie systemów. W ten sposób zbiorcze odzyskiwanie danych na wielu komputerach można przeprowadzić w ciągu kilku minut, a nie godzin lub dni.

- **Szybkie i łatwe odzyskiwanie**

System operacyjny, aplikacje i wszystkie dane można w pełni odzyskać w ciągu kilku minut, a nie godzin lub dni.

- **Odzyskiwanie całego systemu, jednego pliku lub folderu**

Dostępne w oprogramowaniu Acronis funkcje odzyskiwania na podstawie obrazów umożliwiają wybór odpowiedniego stopnia szczegółowości — a przez to szybki powrót do pracy.

- **Program pomocy technicznej i konserwacji Acronis® AdvantageSM**
Acronis® AdvantageSM to rozszerzony, wielopoziomowy, subskrypcyjny program pomocy technicznej i konserwacji. Pierwszy rok korzystania z usług Acronis Advantage jest uwzględniony w cenie licencji.

Główne cechy i funkcje

- **Scentralizowane zarządzanie**

Oparte na zasadach zarządzanie wszystkimi operacjami tworzenia kopii zapasowej i odzyskiwania przy użyciu jednej konsoli.

- **Rozszerzona obsługa środowisk wirtualnych**

Tworzenie kopii zapasowych i odzyskiwanie w środowiskach wirtualnych VMware, Microsoft Hyper-V, Citrix XenServer i Parallels przy użyciu tradycyjnych metod opartych na agentach. Jeśli potrzebne jest bardziej kompleksowe rozwiązanie do tworzenia kopii zapasowych maszyn i środowisk wirtualnych, firma Acronis oferuje również program Acronis® Backup & Recovery™ 10 Advanced Server Virtual Edition.

- **Deduplikacja danych**

Deduplikacja na poziomie plików i bloków pozwala wyeliminować kopie zapasowe identycznych danych i zapewnia znaczną obniżkę kosztów pamięci masowej.

- **Skalowalność**

Obsługa nawet tysięcy komputerów, tworzenie kopii zapasowych w wielu węzłach przechowywania danych.

- **Monitorowanie**

Pulpit roboczy zawiera przegląd wszystkich skonfigurowanych i wykonywanych operacji, wyróżniając procesy wymagające uwagi.

- **Zaawansowane funkcje planowania**

Wykonywanie kopii zapasowych może być uruchamiane po wystąpieniu określonych zdarzeń i warunków.

- **Zaawansowana technologia szyfrowania zapewniająca bezpieczeństwo danych**

Program zawiera dodatkowe warstwy zabezpieczeń, gwarantujące ochronę danych zawartych w kopii zapasowej.

Symantec Backup Exec



Symantec Backup Exec jest aplikacją do tworzenia kopii zapasowych oraz odzyskiwania danych z serwerów i stacji roboczych. Rozwiązanie pozwala na prostą protekcję dużej ilości danych, tym samym obniża koszty pamięci masowej i zwiększa wydajność backup'u dzięki wbudowanemu modułowi deduplikacji i archiwizacji danych.

Dzięki technologii odzyskiwania najważniejszych aplikacji firmy Microsoft oraz wirtualnych środowisk VMware i Microsoft Hyper-V pozwala zredukować do minimum przestoje w działalności firmy. Centralna konsola zarządzająca umożliwia tworzenie kopii zapasowych w środowiskach rozproszonych i zdalnych oddziałach, dzięki temu w miarę rozwoju przedsiębiorstwa bądź instytucji można w bardzo wygodny sposób administrować bezpieczeństwem danych na serwerach oraz stacjach roboczych w jednym miejscu. Program umożliwia również zarządzanie systemami Windows w zestawieniu z innymi platformami takimi jak Linux, UNIX, MAC oraz NetWare, a także zapewniać backup systemów Linux w sieciach SAN. Symantec Backup Exec to oszczędność czasu i kosztów.

Główne zalety:

- dzięki wbudowanym technologiom deduplikacji i archiwizacji danych umożliwia minimalizację kosztów pamięci masowej oraz optymalizację obciążenia sieci,
- innowacyjne rozwiązanie pozwala przywracać informacje na dowolnym stopniu szczegółowości dla oprogramowania SQL i Exchange oraz usługi Active Directory,

- posiada certyfikat Microsoft jako aplikacja do tworzenia backup'u w najnowszych środowiskach, m.in. w systemach Windows 2008 R2, Windows 7, a także programie Exchange 2010,
- kompleksowa funkcjonalność przechowywania informacji na taśmach, dyskach twardych dla najnowszych systemów serwerów fizycznych i wirtualnych (VMware oraz Microsoft Hyper-V),
- mniejsze wymagania odnośnie wielkości zasobów sprzętowych;
- dzięki technologii odtwarzania danych na dowolnym poziomie szczegółowości, skrócony został czas odzyskiwania danych;
- większa wydajność urządzeń obsługiwanych przez protokół NDMP,
- ochrona serwerów opartych na innych systemach niż Windows,
- centralna konsola zarządzająca ułatwia aktualizację infrastruktury oprogramowania Backup Exec z jednego miejsca.

Oracle Secure Backup



Oracle Secure Backup pozwala spełnić wymagania przedsiębiorstwa w zakresie ochrony danych przy wykorzystaniu szyfrowania kopii zapasowych, przechowywania danych na taśmach i zaawansowanej obsługi wirtualnych bibliotek taśm.

Jest to rozwiązanie do scentralizowanego zarządzania kopiami zapasowymi przechowywanymi na taśmach.

- Oferuje ono rozszerzoną obsługę wirtualnej biblioteki taśm (Virtual Tape Library — VTL) z użyciem pozaserwerowego (ang. server-less) powielania taśm, co pozwala poprawić wydajność i ograniczyć obciążenie serwerów podczas kopiowania danych kopii zapasowych z taśm wirtualnych na fizyczne.
- Nowe możliwości zapisu danych na taśmach obejmują bardziej zautomatyzowane zarządzanie taśmami w różnych lokalizacjach. Oprócz standardu IPv4 obsługiwany jest również IPv6. Obsługę platform rozszerzono o systemy HP-UX Itanium, AIX, Linux, Windows i SolarisSPARC.

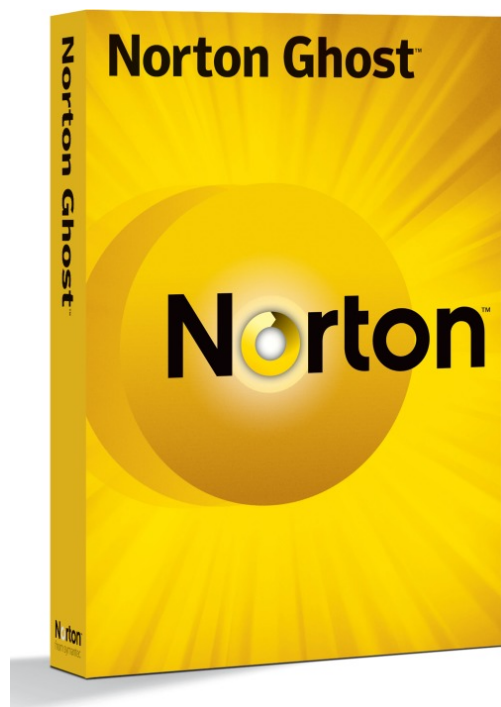
Wszechstronna ochrona danych przedsiębiorstwa

- Oprogramowanie Oracle Secure Backup umożliwia scentralizowane zarządzanie taśmami z kopiami zapasowymi dla baz danych Oracle, systemów plików oraz urządzeń sieciowej pamięci masowej (NAS) z użyciem jednego, wszechstronnego rozwiązania.
- Jest ono oparte na wysoce skalowalnej architekturze klient-serwer, która zapewnia bezpieczeństwo danych przechowywanych na rozproszonych serwerach i urządzeniach sieciowej pamięci masowej, a przy tym oferuje wbudowaną integrację z bazami Oracle Database 11g, Oracle Database 10g i Oracle9i.
- Zoptymalizowana integracja bazy danych, niedostępna w porównywalnych produktach, sprawia, że Oracle Secure Backup pozwala klientom szybciej tworzyć kopie zapasowe bazy danych Oracle na taśmach fizycznych i wirtualnych.
- Rozwiązanie to wykorzystuje protokół NDMP, który podnosi wydajność procesów tworzenia kopii zapasowych i odtwarzania obsługiwanych urządzeń NAS (NetApp, EMC, Pillar Data Systems).
- W oparciu o zaawansowany zestaw funkcji dostępnych także w poprzednich wersjach, Oracle Secure Backup 10.3 pozwala na lepsze wykorzystanie taśm i bardziej zautomatyzowane zarządzanie woluminami, a także na rozwiązywanie trudności związanych z obsługą kopii zapasowych w bardzo rozbudowanych środowiskach.

Nowe funkcje:

- Opcje szyfrowania kopii zapasowych z użyciem hosta lub urządzeń szyfrujących. Rozszerzono możliwości szyfrowania kopii zapasowych. Oprócz dotychczasowej funkcji szyfrowania z wykorzystaniem hosta wprowadzona została obsługa szyfrowania sprzętowego (LTO-4).
- Pozaserwerowe powielanie taśm. Oprócz tradycyjnej metody powielania taśm, rozwiązanie Oracle Secure Backup 10.3 umożliwia powielanie pozaserwerowe. Polega ono na bezpośrednim kopiowaniu taśm wirtualnych na fizyczne z użyciem protokołu NDMP obsługiwanego przez wirtualną bibliotekę taśm.
- Rozszerzone możliwości zapisu danych na taśmach. Jeszcze wyższy poziom automatyzacji zarządzania woluminami i szczegółowości planowania ochrony, możliwość wykonywania zapisu na żądanie, lepsze funkcje raportowania stanu lokalizacji i obsługa wyjątków.

Norton Ghost



Norton Ghost 15.0 umożliwia utworzenie kopii i przywrócenie całego systemu użytkownika oraz wszystkich jego danych - aplikacji, ustawień, folderów i plików. Udostępnia też opcje zdalnego zarządzania kopiami, funkcje szyfrowania i zaawansowanej kompresji. Dzięki programowi Norton Ghost 15.0 użytkownicy mogą szybko przywrócić system po awarii i odzyskać utracone lub uszkodzone pliki, nawet jeśli nie można uruchomić systemu operacyjnego komputera.

Najważniejsze technologie

- Tworzenie obrazów wyłączzonego systemu
- Obsługa dysków Blu-ray
- Tworzenie kopii zapasowych plików i folderów
- Obsługa programu Bitlocker™ w systemie Windows® 7
- Integracja z systemem ThreatCon firmy Symantec
- Zaawansowana kompresja i szyfrowanie
- Tworzenie obrazów wyłączzonego systemu
- Obsługa dysków Blu-ray
- Tworzenie kopii zapasowych plików i folderów
- Obsługa programu Bitlocker™ w systemie Windows® 7
- Integracja z systemem ThreatCon firmy Symantec
- Zaawansowana kompresja i szyfrowanie
- Przyrostowe aktualizacje kopii zapasowej

- Kopie zapasowe tworzone na podstawie zdarzeń
- Tworzenie kopii zapasowych w lokalizacjach wewnętrznych i zewnętrznych
- Tworzenie pełnej kopii zapasowej i przywracanie systemu (obraz dysku)

Główne zalety

- Tworzenie pełnych kopii zapasowych systemu i poszczególnych plików — ochrona systemu, ustawień, aplikacji i plików dzięki elastycznej i kompleksowej ochronie wykonywania kopii zapasowych.
- Przywracanie systemu w przypadku awarii — odtwarzanie systemu i danych nawet w przypadku braku możliwości ponownego uruchomienia komputera.
- Wygodne i bezpieczne tworzenie kopii zapasowych w innych lokalizacjach — zapisywanie punktów odtwarzania w serwerze FTP w celu ułatwienia zarządzania nimi poza siedzibą firmy, a nawet wykonywanie kopii zapasowych danych w urządzeniach pamięci masowej podłączonych do sieci.
- Tworzenie pełnych kopii zapasowych systemu i poszczególnych plików — ochrona systemu, ustawień, aplikacji i plików dzięki elastycznej i kompleksowej ochronie wykonywania kopii zapasowych.
- Przywracanie systemu w przypadku awarii — odtwarzanie systemu i danych nawet w przypadku braku możliwości ponownego uruchomienia komputera.
- Wygodne i bezpieczne tworzenie kopii zapasowych w innych lokalizacjach — zapisywanie punktów odtwarzania w serwerze FTP w celu ułatwienia zarządzania nimi poza siedzibą firmy, a nawet wykonywanie kopii zapasowych danych w urządzeniach pamięci masowej podłączonych do sieci.
- Wykonywanie kopii zapasowych według harmonogramów i po wystąpieniu określonych zdarzeń — możliwość wybierania danych uwzględnianych w kopii zapasowej oraz czasu jej tworzenia, dzięki czemu można dostosować proces wykonywania kopii zapasowych do sposobu korzystania z komputera.

Funkcje

- Tworzenie obrazów wyłączzonego systemu — wykonywanie kopii zapasowych plików bez konieczności instalacji programu Ghost.
- Obsługa dysków Blu-ray umożliwia tworzenie kopii zapasowych dużych ilości danych na dyskach Blu-ray o dużej pojemności — do 25 GB na każdym dysku (50 GB w przypadku dysków dwuwarstwowych).
- Obsługa technologii Bitlocker™ w systemie Windows® 7 — zaawansowana ochrona danych przez stosowanie szyfrowania i sprawdzanie integralności.
- Tworzenie obrazów wyłączzonego systemu — wykonywanie kopii zapasowych plików bez konieczności instalacji programu Ghost.
- Obsługa dysków Blu-ray umożliwia tworzenie kopii zapasowych dużych ilości danych na dyskach Blu-ray o dużej pojemności — do 25 GB na każdym dysku (50 GB w przypadku dysków dwuwarstwowych).
- Obsługa technologii Bitlocker™ w systemie Windows® 7 — zaawansowana ochrona danych przez stosowanie szyfrowania i sprawdzanie integralności.

- Integracja z systemem ThreatCon firmy Symantec — wykorzystanie informacji pochodzących z jednej z najlepszych w branży organizacji firmy Symantec zajmującej się badaniami zabezpieczeń w celu automatycznego tworzenia kopii zapasowych w chwili, gdy stopień zagrożenia ThreatCon osiągnie określony poziom.
- Pełna kopia zapasowa systemu (obraz dysku) umożliwia tworzenie kopii zapasowych wszystkich zasobów znajdujących się na dysku twardym lub partycji.
- Tworzenie kopii zapasowych plików i folderów — możliwość archiwizowania tylko wybranych plików i katalogów zamiast zapisywania zawartości całego dysku twardego.
- Wyszukiwanie plików dla kopii zapasowych — wyszukiwanie i wykonywanie kopii zapasowej tylko wybranych typów plików, takich jak zdjęcia, pliki MP3 czy dokumenty.
- Tworzenie przyrostowych kopii zapasowych — kopiowanie tylko zmodyfikowanych plików, co przyspiesza tworzenie kopii zapasowych i ogranicza jego częstotliwość.
- Tworzenie kopii zapasowych na podstawie zdarzeń z możliwością dostosowania do własnych potrzeb — wykonywanie kopii zapasowych inicjowane w przypadku wystąpienia ważnych zdarzeń, takich jak instalacja nowego programu lub nagły wzrost zużycia pamięci masowej.
- Tworzenie kopii zapasowych w innych lokalizacjach — kopiowanie punktów odtwarzania na serwer FTP w celu ułatwienia zarządzania kopiami zapasowymi poza siedzibą organizacji.
- Tworzenie kopii zapasowych w urządzeniach NAS — wykonywanie kopii zapasowych plików w urządzeniach pamięci masowej podłączonych do sieci.
- Zaawansowana kompresja — automatyczna kompresja plików w celu zmniejszenia ilości miejsca zajmowanego na dysku.
- Zaawansowane szyfrowanie — ochrona poufnych dokumentów przez ukrywanie ich przed osobami pragnącymi uzyskać do nich dostęp.
- Ochrona systemu — łatwiejsze przywracanie systemu, aplikacji i plików nawet w sytuacji, gdy niemożliwe jest ponowne uruchomienie systemu operacyjnego.
- Integracja z programem Google Desktop™ — jeszcze szybsze odzyskiwanie danych dzięki indeksom kopii zapasowych z możliwością przeszukiwania.
- Funkcja LightsOut Restore — szybkie przywracanie systemu bez konieczności używania rozruchowego dysku CD.
- Zdalne zarządzanie — kontrolowanie innych instalacji programu Norton Ghost (w wersji 12.0 lub nowszej) w sieci lokalnej.
- Zaplanowana konwersja systemów fizycznych na wirtualne (P2V) — możliwość automatycznego tworzenia dysku wirtualnego z najnowszej kopii zapasowej.
- Obsługa wersji umożliwia przywracanie danych na podstawie starszych wersji obrazów dysku utworzonych przy użyciu programu Ghost w wersji 10, 12 i 14.

- Obsługa wielu modułów pamięci masowej — możliwość tworzenia kopii zapasowych niemal na wszystkich nośnikach, między innymi na dyskach Blu-ray®, CDR/RW i DVD+-R/RW, urządzeniach USB i FireWire® (IEEE 1394), dyskach sieciowych oraz napędach Iomega® Zip® i Jaz®.